Diskrete Logarithmen - Was ist denn das?

Dr. Detlef Zerfowski, (Bangalore, Indien)
Version von 12. Mai 2013.

1 Von gewöhnlichen zu diskreten Logarithmen

Gewöhnliche Logarithmen sind den meisten von uns aus der Schule bekannt. Ich kann mich noch an meine eigene Schulzeit erinnern, in der viele meiner Schulfreunde mit den logarithmischen Berechnungen erhebliche Schwierigkeiten und heftig zu kämpfen hatten. Diejenigen die sich mit Rechenschiebern befassen oder befasst haben, können die in der Analysis verwendeten Logarithmen keine Ängste einjagen. Mit diesem Aufsatz möchte ich dasselbe für die diskreten Logarithmen erreichen.
Den Weg von den gewöhnlichen zu den diskreten Logarithmen gehen wir schrittweise an:

i. Zuerst müssen wir einen kleinen Exkurs in die Mathematik machen und uns die Eigenschaften von Zahlenmengen genauer anschauen.

ii. Dann werden wir feststellen, welche dieser Eigenschaften erforderlich sind und welche überraschenderweise nicht, um Logarithmen berechnen zu können.

iii. Schließlich werden wir neue Zahlenmengen mit den erforderlichen Eigenschaften kennenlernen und in diesen Zahlenmengen diskrete Logarithmen berechnen.

iv. Abschließend gehen wir auf einige praktische Anwendungen der diskreten Logarithmen ein. Insbesondere werden Sie erfahren, warum die diskreten Logarithmen auf ihr Geld aufpassen.

2 Eigenschaften von Zahlenmengen

2.1 Eigenschaften der reellen Zahlen

Aber beginnen wir zur Aufwärmung mit der altbekannten Analysis, die ein Teilgebiet der Mathematik ist. Zur Erinnerung: die Analysis befasst sich mit Funktionen über den reellen Zahlen. Die Menge der reellen Zahlen, die auch mit dem Symbol $\mathbb{R}$ bezeichnet wird, ist die Menge aller Punkte der Zahlengerade. Die Logarithmus- und Exponentialfunktionen sind Funktionen die auf der Menge der reelen Zahlen $\mathbb{R}$ operieren.

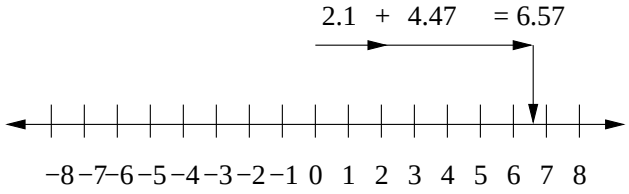

Abbildung 1: Addition auf der Zahlengerade.

Betrachten wir aber erst einmal die Menge $\mathbb{R}$ und einige ihrer Eigenschaften, die wir im täglichen Rechnen implizit verwenden. Häufig ist man sich dieser Eigenschaften und ihrer Bedeutungen gar nicht bewusst.
Betrachten wir einige dieser Eigenschaften der reellen Zahlen $\mathbb{R}$.

Eigenschaft 1: Unendlich große Menge
Es gibt unendlich viele reelle Zahlen.

Eigenschaft 2: Zahlengerade 1
Jede reelle Zahlen lässt sich als ein Punkt auf einem Zahlengerade darstellen

Eigenschaft 3: Zahlengerade 2
Jeder Punkt auf der Zahlengerade entspricht einer reellen Zahl.

Eigenschaft 4: Abgeschlossenheit der Addition
Bei der Addition zweier reeller Zahlen erhält man als Ergebnis stets eine reelle Zahl (z.B. $2,1 + 4,47 = 6,57$).

Eigenschaft 5: Abgeschlossenheit der Subtraktion
Bei der Subtraktion zweier reeller Zahlen erhält man als Ergebnis stets eine reelle Zahl (z.B. $6,57 - 4,47 = 2,1$).

Eigenschaft 6: Abgeschlossenheit der Mulitplikation
Bei der Multiplikation zweier reeller Zahlen erhält man wiederum eine reelle Zahl.

Eigenschaft 7: Abgeschlossenheit der Division
Bei der Division zweier reeller Zahlen erhält man wiederum eine reelle Zahl.

Eigenschaft 8: Abgeschlossenheit des Potenzierens
Bei der Potenzierung einer reellen Zahl mit einer anderen reellen Zahl erhält man wiederum eine reelle Zahl.

Eigenschaft 9: Abgeschlossenheit des Logarithmierens
Beim Logarithmieren einer reellen Zahlen (zur Basis einer reellen Zahl) erhält man wiederum eine reelle Zahl.

Sie meinen vielleicht, dass dies doch selbstverständlich und langweilig ist. Dem ist aber nicht so!

2.2 Eigenschaften der ganzen und natürlichen Zahlen

Betrachten Sie z.B. die Menge der ganzen Zahlen, die mit dem Symbol $\mathbb{Z}$ abgekürzt wird. Diese Menge $\mathbb{Z}$ umfasst alle negativen und positiven ganzen Zahlen inklusive der Null (also $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$).
Welche der oben genannten 9 Eigenschaften treffen auf die Menge der ganzen Zahlen zu?
Wenn Sie es selber herausfinden wollen nehmen Sie jetzt ein Blatt Papier, schreiben die obigen Eigenschaften 1 bis 9 für die Menge der ganzen Zahlen auf und überprüfen, ob die Aussagen stimmen. Lesen Sie erst danach weiter.
Nachfolgend finden Sie die Lösung der Aufgabe:
Für die Menge $\mathbb{Z}$ der ganzen Zahlen gelten die Eigenschaften 1, 2, 4, 5, 6. Für die anderen Eigenschaften, angewandt auf die Menge der ganzen Zahlen, ergibt sich:

> **Eigenschaft 3** gilt nicht, da nicht jeder Punkt der Zahlengerade eine ganze Zahl darstellt.
>
> **Eigenschaft 7** gilt nicht, da bei der Division zweier ganzer Zahlen sehr oft keine ganze Zahl als Ergebnis auftritt. (z.B. $2/5 = 0,4$ was offensichtlich keine ganze Zahl ist).
>
> **Eigenschaft 8** gilt nicht, da beim Potenzieren einer ganzer Zahlen mit einer anderen ganzen (negativen) Zahl sehr oft keine ganzen Zahlen als Ergebnis auftritt. (z.B. $5^{-2} = \frac{1}{5^2} = \frac{1}{25}$ was offensichtlich keine ganze Zahl ist).
>
> **Eigenschaft 9** gilt nicht, da z.B. für $2^x = 10$ die Zahl x offensichtlich keine ganze Zahl ist.

Für die Menge $\mathbb{N}$ der natürlichen Zahlen, das sind die ganzen Zahlen größer als Null, verliert eine weitere Eigenschaft ihre Gültigkeit. Die Eigenschaft 5 (Abgeschlossenheit der Subtraktion) gilt nicht mehr, denn z.B. $2 - 5 = -3$ und -3 gehört nicht mehr zu den positiven ganzen Zahlen.
Aber man beachte: Für $\mathbb{N}$ ist die Eigenschaft 8 plötzlich wieder gültig! Jede natürliche Zahl potenziert mit einer belieben natürlichen Zahl ergibt wieder eine natürliche Zahl. Das liegt daran, dass die Exponenten nur ganze Zahlen größer Null sein dürfen.

3 Welche Eigenschaften benötigt man zum Berechnen von Logarithmen?

Im vorherigen Abschnitt haben wir einige bemerkenswerte Eigenschaften bzw. Nicht-Eigenschaften von Zahlenmengen kennen gelernt.
Es stellt sich nun die Frage welche dieser Eigenschaften sind erforderlich, dass man in der entsprechenden Zahlenmenge Logarithmen berechnen kann? Und welche Eigenschaften benötigt man nicht?
Ohne die Abgeschlossenheit der Subtraktion (Eigenschaft 5) wird es bereits schwierig eine Division zu realisieren. Eine Division kann als wiederholte Subtraktion durchgeführt werden, wie dies auch mechanischen Vierspeziesrechenmaschinen geschieht.
Auf den ersten Blick scheint es, dass alle neun Eigenschaften benötigt werden. Bei der Verwendung von gewöhnlichen Logarithmen verwendet man, ohne großes Nachdenken, die Menge der reellen Zahlen und damit implizit die Eigenschaften der Zahlengerade. Dies ist besonders deutlich bei der Verwendung von Rechenschiebern, die in verschiedenen Ausprägungen Abschnitte unterschiedlicher Zahlengeraden (Skalen) verwenden.
Und hier liegt die Überraschung: Um Logarithmen berechnen zu können werden die Eigenschaften 4 bis 9 benötigt, aber nicht die Eigenschaften 1 bis 3!
Es ist aber eine weitere Eigenschaft erforderlich, um in einer Menge den Logarithmus definieren zu können.

Eigenschaft 10: Erzeugendes Element der Menge
Es gibt eine Zahl w mit der man jede beliebige Zahl a der Menge erreichen kann, indem es eine Zahl b gibt, so dass $w^b = a$ ist.

Sie mögen sich wundern, was dies für eine seltsame Eigenschaft ist. Wiederum handelt es sich dabei um eine Eigenschaft, die Sie beim Rechnen mit Logarithmen in den reellen Zahlen, implizit nutzen. In den reellen Zahlen gibt es unendlich viele Zahlen die Sie als Basis Logarithmenbasis w verwenden können.
Es gibt jedoch Zahlenmengen, bei denen es nur wenige Elemente gibt, die die Eigenschaft 10 erfüllen und genau diese werden wir uns im weiteren Verlauf anschauen.
Es gibt Mengen, bestehend aus endlich vielen Zahlen, die man nicht auf einer Zahlengerade anordnen kann, für die man jedoch abgeschlossene mathematische Operation für Addition, Subtraktion, Multiplikation, Division, Potenzieren und Logarithmieren, sowie mindestens ein erzeugendes Element angeben kann.
Die Logarithmen in diesen endlichen Zahlenmengen sind die sogenannten diskreten Logarithmen.
Um die Berechnung der diskreten Logarithmen zu verstehen, müsssen wir uns die entsprechenden Mengen und die Definition der mathematischen Operationen detaillierter anschauen.
Betrachten wir eine Menge K von Zahlen[1] mit den mathemischen Operationen "+" und "*".
Folgende Eigenschaften sollen für beliebige Zahlen a, b, c aus der Menge K gelten:

K1: Assoziativgesetz der Addition
$a + (b + c) = (a + b) + c$

K2: Kommutativgesetz der Addition
$a + b = b + a$

K3: Neutrales Element bzgl. Addition (Null)
Es gibt eine Zahl 0 in der Menge K, für das gilt $0 + a = a$.

K4: Inverses Element bzgl. Addition (Subtraktion)
Für jede Zahl a in der Menge K, gibt es eine Zahl $-a$, für das gilt $(-a) + a = 0$.

K5: Assoziativgesetz der Multiplikation
$a * (b * c) = (a * b) * c$

K6: Kommutativgesetz der Multiplikation
$a * b = b * a$

[1] Man kann hier auch beliebige Elemente nehmen. Um es aber nicht zu abstrakt werden zu lassen, bleiben wir bei Zahlen

K7: Neutrales Element bzgl. Multiplikation (Eins)
Es gibt eine Zahl 1 in der Menge K, für die für alle $a \neq 0$ gilt: $1 * a = a$.
(Hinweis: Der Korrektheit wegen muss auch noch $1 \neq 0$ gefordert werden, worauf wir nicht weiter eingehen.)

K8: Inverses Element bzgl. Multiplikation (Division)
Für jede Zahl a in der Menge K, gibt es eine Zahl a^{-1}, für das gilt $a^{-1} * a = 1$.

K9: Distributivgesetz
$a * (b + c) = a * b + a * c$

K10: Erzeugendes Element
Es gibt mindestens eine Zahl w, für die jede beliebige Zahl $a \neq 0$ eine Zahl b existiert, so dass $w^b = a$ gilt.

Mit den Eigenschaften K1 bis K10 haben wir das Rüstzeug, um uns den diskreten Logarithmen zu zuwenden. Schauen Sie sich die Eigenschaften nochmals aus der Sicht der reellen Zahlen an. Ersetzen dazu einfach die Menge K durch die Menge der reellen Zahlen $\mathbb{R}$.
Insbesondere die etwas ungewöhnlich erscheinende Eigenschaft "Erzeugendes Element" wird im weiteren Verlauf eine wesentliche Rolle spielen.

4 Primzahlkörper und wie man darin rechnet

Wer es bis zu dieser Stelle des Artikels geschafft hat, der hat das Schwierigste überwunden. Wir werden nun für die Zahlenmenge K eine endliche Zahlenmenge angeben und die zugehörigen Operationen für Addition und Multiplikation festlegen.
Es gibt sehr viele endliche Zahlenmengen (genauer gesagt sogar unendlich viele), die sogenannten Primzahlkörper, die die oben genannten Eigenschaften K1 bis K10 erfüllen.
Wir gehen davon aus das p eine Primzahl sei, d.h. p ist ganze Zahl größer als 1, die nur durch 1 und sich selbst teilbar ist. Beispiele für Primzahlen sind 2 (die einzige gerade Primzahl), $3, 5, 7, 11, \ldots, 101, \ldots$
Für einen Primzahlkörper zur Primzahl p betrachtet man nur noch alle ganzen Zahlen von 0 bis $p - 1$.
Für das Beispiel $p = 11$ betrachten wir somit nur die Menge der Zahlen $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
Damit die Addition zweier beliebigen Zahlen aus dieser Menge wieder eine Zahl dieser Menge ist, definiert man die folgende Regeln.

4.1 Addition im Primzahlkörper

Zwei beliebige Zahlen a und b werden folgendermaßen addiert. Berechne $c = a + b$ wie gewohnt und berechne dann aus diesem Zwischenergebnis den ganzzahligen Rest der bei der Division durch p übrigbleibt.
Durch die letzte Operation ist sichergestellt, dass das Endergebnis c (der ganzzahlige Rest) stets im Bereich 0 bis $p - 1$ liegt.
Als Formel schreibt man dieses so $a + b \equiv c \mod 11$ (sprich: a plus b ist kongruent c modulo 11).
Bei dieser Art der Rechnung lässt sich also nicht mehr zwischen den Zahlen a und $a + p$ unterscheiden, da beide bei Division durch p den selben Rest ergeben.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Dann gilt $a + b = 16$. Nun berechnet man 16 geteilt durch 11 und erhält $16/11 = 1$ Rest 5. Das Endergebnis lautet 5, oder in Formelschreibweise $7 + 9 \equiv 5 \mod 11$ (vgl. die Abbildung 2 zur Addition auf dem Zahlenkreis).

4.2 Subtraktion im Primzahlkörper (Inverses bzgl. Addition)

Zwei beliebige Zahlen a und b werden folgendermaßen subtrahiert. Berechne $a - b$ wie gewohnt, falls das Ergebnis kleiner 0 ist, addiere Vielfache von p auf, so dass das Ergebnis größer oder gleich 0 und berechne dann aus diesem Zwischenergebnis den ganzzahligen Rest der bei der Division mit p bleibt.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Dann gilt $a - b = -2$. Nun berechnet man $-2 + 11 = 9$ und teilt dies durch 11 und erhält $9/11 = 0$ Rest 9. Das Endergebnis lautet 9, oder in Formelschreibweise $7 - 9 \equiv 9 \mod 11$.
Trägt man die Zahlen $0, \ldots, p-1$ auf einem Ring auf, so lässt sich die Addition bzw. Subtraktion grafisch einfach veranschaulichen, wenn man entsprechend viele Einheiten im bzw. entgegen dem Uhrzeigersinn weitergeht.

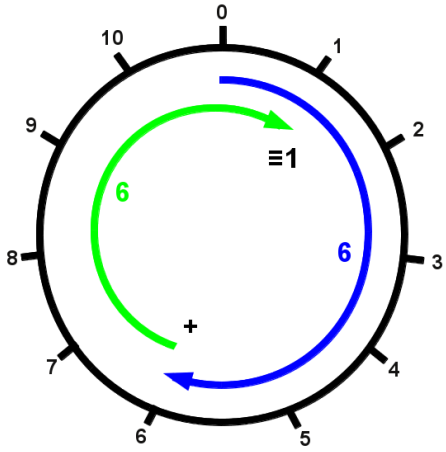

Abbildung 2: Addition $6 + 6 \equiv 1 \mod 11$ am Zahlenkreis.

4.3 Multiplikation im Primzahlkörper

Zwei beliebige Zahlen a und b werden folgendermaßen multipliziert. Berechne $a * b$ wie gewohnt und berechne dann aus diesem Zwischenergebnis den ganzzahligen Rest der bei der Division durch p übrigbleibt.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Dann gilt $a * b = 63$ und teilt dies durch 11 und erhält $63/11 = 5$ Rest 8. Das Endergebnis lautet 8, oder in Formelschreibweise $7 * 9 \equiv 8 \mod 11$.

4.4 Division im Primzahlkörper (Inverses bzgl. Multiplikation)

Die Division ist nicht ganz so einfach zu verstehen. In der Menge der ganzen Zahlen $0, \ldots, p-1$ gibt es ja keine Brüche, die wir von den reellen Zahlen kennen. Betrachten wir die Division bei reellen Zahlen etwas genauer. Wollen wir eine reelle Zahl a durch eine reelle Zahl b teilen, so kann man dies auf eine Multiplikation zurückführen: Statt a/b zu berechnen kann man a mit der Zahl b^{-1} multiplizieren, wobei für b und b^{-1} gelten muss, dass $b * b^{-1} = 1$ ist (Eigenschaft K8 "Inverses Element bzgl. Multiplikation").
Sie werden jetzt sagen, dass dies banal ist. Ob ich für $a = 3$ und $b = 4$ die Division $a/b = 3/4 = 0.75$ rechne oder $a * b^{-1} = 3 * 0,25 = 0,75$ rechne (Beachte $b * b^{-1} = 4 * 0,25 = 1$) ist doch gleichgültig! Dieses stimmt für die reellen Zahlen, aber nicht für die Primzahlkörper!
Bei Primzahlkörpern muss man zuerst b^{-1} bestimmen und dann die Multiplikation mit diesem b^{-1} durchführen. Durch dieses Vorgehen ist sichergestellt, dass das Ergebnis wieder eine ganze Zahl im Bereich 0 bis $p-1$ ist.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Um $a * b^{-1}$ zu berechnen, muss zuerst b^{-1} berechnet werden. Für $b = 9$ gilt $b^{-1} = 5$, denn $b * b^{-1} = 9 * 5 = 45 \equiv 1 \mod 11$. Die Division wird somit durch die Multiplikation $a * b^{-1} = 7 * 5 = 35 \equiv 2 \mod 11$ berechnet.

Darauf, dass die restlichen Eigenschaften K1 bis K9 mit den obigen Operationen erfüllt sind, gehen wir hier nicht detaillierter ein. Der Leser kann dieses mit Hilfe des abgebildeten Zahlenkreises in Abbildung 2 selber überprüfen.
Wir wollen uns nun auf die Eigenschaft K10 "Erzeugendes Element" konzentrieren, da diese der zentrale Punkt für die Definition des diskreten Logarithmus ist.

4.5 Primitive Wurzel im Primzahlkörper (Erzeugendes Element)

Betrachtet man eine beliebige reelle Zahl a ungleich 0, so kann man bei einer fest vorgegebenen Basis, zum Beispiel der Zahl 3, die Zahl a durch einen eindeutigen Exponenten x ausdrücken, so dass $a = 3^x$ gilt.
Eine ähnliche Bedeutung wie im Beispiel die Zahl 3, besitzt die sogenannte primitive Wurzel (das erzeugende Element) in Primzahlkörpern. Bezeichnen wir eine primitive Wurzel mit w, so kann man alle Zahlen 1 bis $p-1$ im Primzahlkörper durch mehrfaches Multiplizieren von w mit sich selbst erzeugen. Das heißt, jede Zahl a kann in der Form w^i geschrieben werden. Der Exponent i wird als Index oder besser als **diskreter Logarithmus** bezeichnet!
Endlich haben wir unser Etappenziel, die Definition des diskreten Logarithmus erreicht.

Beispiel für $p = 11$:

Eine primitive Wurzel für den Primzahlkörper der Primzahl $p = 11$ ist $w = 2$, denn

$$\begin{aligned}
w^0 &= 2^0 = 1 &&\equiv 1 \mod 11\\
w^1 &= 2^1 = 2 &&\equiv 2 \mod 11\\
w^2 &= 2^2 = 4 &&\equiv 4 \mod 11\\
w^3 &= 2^3 = 8 &&\equiv 8 \mod 11\\
w^4 &= 2^4 = 16 &&\equiv 5 \mod 11\\
w^5 &= 2^5 = 32 &&\equiv 10 \mod 11\\
w^6 &= 2^6 = 64 &&\equiv 9 \mod 11\\
w^7 &= 2^7 = 128 &&\equiv 7 \mod 11\\
w^8 &= 2^8 = 256 &&\equiv 3 \mod 11\\
w^9 &= 2^9 = 512 &&\equiv 6 \mod 11
\end{aligned}$$

Man beachte, dass alle Zahlen von 1 bis $10 (= p-1)$ als Ergebnis auftreten. Desweiteren beachte man, dass mit jeder weiteren Multiplikation mit $w = 2$ sich die Ergebnisse wiederholen, z.B.

$$w^{10} = 2^{10} = 1024 \equiv 1 \mod 11 \quad \text{und} \quad w^{11} = 2^{11} = 2048 \equiv 2 \mod 11.$$

Aus der vorhergehenden Übersicht lässt sich somit für jede Zahl von 1 bis $p-1$ der diskrete Logarithmus direkt ablesen. Z.B. ist für 10 der diskrete Logarithmus die 5 (da $2^5 \equiv 10 \mod 11$). Dabei ist zu beachten, dass als Exponenten nur die Zahlen 0 bis $p-2$ auftreten, da man die Zahl 0 nicht als Potenz w^i darstellen kann[2]. Im Exponenten muss man also stets den Rest bei der Division mit $p-1$ berechnen, nicht den Rest bei der Division mit p!

4.6 Multiplikation mit diskreten Logarithmen

Jetzt können wir Multiplikation im Primzahlkörper mit diskreten Logarithmen durchführen. Die Multiplikation zweier Zahlen a und b im Primzahlkörper, lässt sich analog zu den reellen Zahlen als Addition der diskreten Logarithmen berechnen.

[2]Dies gilt auch für Logarithmen über den reellen Zahlen.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Die diskreten Logarithmen von a bzw. b sind 7 bzw 6. Die Addition der Exponenten liefert $6 + 7 = 15$. Da es sich um Exponenten handelt muss man hier den Rest bzgl. Division mit $p - 1$, also 10 bestimmen. Das heißt, der diskrete Logarithmus des Endergebnis ist $6 + 7 = 13 \equiv 3 \mod 10$. Schaut man wieder in die Tabelle, dann erkennt man, dass $w^3 = 23 = 8 \equiv 8 \mod 11$ (jetzt wieder 11, da man nicht im Exponenten rechnet) ist und somit 8 das Endergebnis ist. Dieses stimmt mit dem Ergebnis im Beispiel des Abschnitts "Multiplikation im Primzahlkörper" überein.

4.7 Division im Primzahlkörper mit diskreten Logarithmen

Gleiches wie bei der Multiplikation gilt auch für die Division. Analog zu den reellen Zahlen, wo eine Division durch Subtraktion der Logarithmen erfolgen kann, wird dies im Falle der Primzahlkörper durch die Subtraktion der diskreten Logarithmen realisiert. Bei dieser Subtraktion wird wieder mit den Resten der Division mit $p - 1$ gerechnet, nicht mit p.

Beispiel für $p = 11$:

Sei $a = 7, b = 9$. Um $a * b^{-1}$ zu berechnen, muss zuerst b^{-1} berechnet werden. Für $b = 9$ gilt $b^{-1} = 5$, denn $b*b^{-1} = 9*5 = 45 \equiv 1 \mod 11$. Die Division $a*b^{-1}$ wird nun durch die Multiplikation $a*b^{-1} = 7*5 = 35 \equiv 2 \mod 11$ berechnet.

4.8 Exponentiation im Primzahlkörper mit diskreten Logarithmen

Entsprechend der Regeln für reellen Zahlen, lässt sich dieses im Primzahlkörper durch Multiplikation des diskreten Logarithmus $\mod p - 1$ bewerkstelligen.

4.9 Wurzelziehen im Primzahlkörper mit diskreten Logarithmen

Analog zur Exponentiation kann man durch Division des diskreten Logarithmus $\mod p - 1$ radizieren. Aber Achtung: Da $p - 1$ keine Primzahl ist, funktioniert der im Abschnitt "Division im Primzahlkörper" angegebene Trick mit der Multiplikation mit b^{-1} nicht bei jeder Zahl. Es gibt also nicht für jede Zahl b aus $0, \ldots, p - 2$ eine Zahl b^{-1} mit der Eigenschaft $b * b^{-1} \equiv 1 \mod p - 1$. In den Fällen wo es kein geeignetes b^{-1} gibt, exisitiert keine entsprechende Wurzel.

5 Schumachers Rechenschieber mit diskreten Logarithmen

Sie mögen sich nun fragen, wofür braucht man denn die diskreten Logarithmen. Das ist doch nur graue Theorie und ohne praktische Bedeutung. Wenn Sie so denken begehen Sie den selben Fehler, dem auch andere Personen unterliegen, die aktuell die Logarithmenrechnungen aus den Lehrplänen deutscher Schulen entfernen wollen oder entfernt haben.
In diesem Abschnitt gehen wir auf eine wenig beachtete, historische Anwendung der diskreten Logarithmen im Rechenschieberbereich ein. Zugegebener Maßen handelt es sich dabei eher um eine Anwendung aus dem universitärem Bereich zu Beginn des letzten Jahrhunderts.
Im nächsten Kapitel kommen wir aber darauf zu besprechen, welche Bedeutung die diskreten Logarithmen heute im täglichen Leben haben.
Aber kehren wir ein wenig in die Vergangenheit zurück. Im Jahr 2004 traf ich während eines Bodenseeurlaubs den Sammlerfreund und Rechenschieberexperten Heinz Joss zu einem gemeinsamen Mittagessen. Während des Essens erwähnte er einen außergewöhnlichen Rechenschieber von Faber-Castel nach dem System Schumacher. Niemand in der Sammlergemeinde konnte etwas mit dem Gerät anfangen und Dieter von Jezierski, der im Besitz eines entsprechenden Exemplars war, wollte bereits einen Artikel über die Sinnlosigkeit des Rechenschiebers verfassen. Aufgrund der Beschreibungen von Heinz Joss und meiner Kenntnisse in der diskreten Algebra wurde ich hellhörig und vermutete eine echte Rarität: ein Rechenschieber mit diskreten Logarithmen.

Dieter von Jezierski, Paul Weinmann und ich verfassten einen entsprechenden Artikel [JezWeiZer2004] im Journal of the Oughtred Society, der die Funktionsweise des Rechenschiebers erklärte.
Schumachers Rechenschieber verwendet im Gegensatz zu den zuvor angegebenen Beispielen mit $p = 11$ die Primzahl $p = 101$. In einem separaten Quadrat auf dem Rechenschieber hat er die diskreten Logarithmen der Zahlen $1, \ldots, 100$ angegeben. In dem Quadrat findet man z.B. den diskreten Logarithmus x von 16 in dem man in der Zeile mit der führenden 1 und der Spalte 6 nach schaut. Man findet dort die 4. Es gilt $w^4 = 2^4 \equiv 16 \mod 101$.
Um den diskreten Logarithmus von 99 zu finden geht man in Zeile 9 und Spalte 9 und findet den Wert 51. Es gilt $w^{51} = 2^{51} \equiv 99 \mod 101$. Rechnen Sie es selber nach: 2^{51} liefert nach Division durch die Primzahl 101 den Rest 99.

Abbildung 3: Tabelle der diskreten Logarithmen mod 101 von Schumachers Rechenschieber.

Ein Vorteil der Verwendung von $p = 101$ ist, dass die Resteberechnung mod $p - 1$, also mod 100, sehr einfach im Kopf geschehen kann, da man nur die letzten zwei Ziffern der jeweiligen Ergebnisse berücksichtigen muss.
Es stellt sich die Frage wie die oben dargestellten Rechenoperationen in der Praxis auf dem Rechenschieber anwendbar waren. Man darf hierzu nicht die Anforderungen stellen, die man an einen Rechenschiebereinsatz im Ingenieurswesen stellt. Herr Schumacher kommt nicht aus den Ingenieursdisziplinen, sondern aus der Mathematik. In seine Dissertation "Zur Theorie der biquadratischen Gleichungen" [Sch1884] an der Universität Erlangen aus dem Jahre 1884 behandelte er biquadratische Gleichungen, bei denen es um ganzzahlige Lösungen derselben geht. Dabei ist es zwingend erforderlich, dass die Ergebnisse exakt sein müssen. Angenäherte Rechenergebnisse machen für diese Problemklassen keinen Sinn. Für solche Art mathematischer Probleme sind herkömliche Rechenschieber denkbar ungeeignet, da man aufgrund der Ungenauigkeiten beim Ablesen, nie genau sagen kann, ob das Ergebnis wirklich ganzzahlig ist, oder vielleicht doch um einen Bruchteil neben einer ganzen Zahl liegt.
Schumachers Rechenschieber hatte somit eine völlig andere Zielgruppe im Blick als die Nutzer herkömmlicher Rechenschieber, nämlich Mathematiker, die sich mit mathematischen Problemen über ganzen Zahlen beschäftigen. Er konnte und sollte auch nicht den herkömmlichen Rechenschieber ersetzen.
Die Grundlagen für die benötigten Theorien wurden durch Mathematiker wie Jacobi geschaffen, den Schumacher in seiner Beschreibung explizit erwähnt. Genau für Mathematiker, die sich mit diesen Theorien beschäftigt haben, konnte der Rechenschieber eine Hilfe sein.

5.1 Dezimale Darstellung ganzer Zahlen

Um eine breitere Nutzung des Rechenschiebers zu ermöglichen, gibt Schumacher eine Reihe von mathematischen Rechentricks an, mit denen man auch für größere Zahlen den Rechenschieber verwenden konnte. Dabei wurden jedoch nicht die Eigenschaften von Primzahlkörpern genutzt, sondern spezielle Eigenschaften der Zahl 101 und dem Zehnersystem (Dezimalsystem) unserer Schreibweise von Zahlen.
Unsere Art Zahlen aufzuschreiben, ist eine abkürzende Schreibweise. In der Grundschule lernten wir noch das Zahlen aus "Einern", "Zehnern", "Hunderten", "Tausendern", usw. bestehen. Die Zahl 7489 z.B. kann auch in der Form

$$7489 = 7 \text{ Tausender } +4 \text{ Hunderter } +8 \text{ Zehner } +9 \text{ Einer}$$

geschrieben werden. Die "Einer", "Zehner", "Hunderter", "Tausender", usw. sind aber nichts anderes als $10^0, 10^1, 10^2, 10^3$, usw. also x^i für $x = 10$ (beginnend mit $i = 0$).
Die Zahl 7489 kann somit auch wie folgt geschrieben werden:

$$7489 = 7 * 10^3 + 4 * 10^2 + 8 * 10^1 + 9 * 10^0 = 7 * x^3 + 4 * x^2 + 8 * x^1 + 9 * x^0 \text{ für } x = 10.$$

Statt für $x = 10$ (Zehnerdarstellung) kann man auch die Darstellung für $x' = 100$ verwenden (Hunderterdarstellung)

$$7489 = 74 * 100^1 + 89 * 10^0 = 74 * x'^1 + 89 * x'^0 \text{ für } x' = 100.$$

Da Schumacher mit seinem Rechenschieber wegen der Wahl von $p = 101$ auch leicht die Reste $\mod 100$ bestimmen konnte, war es ihm unter Verwendung einiger "Rechenkniffe" möglich auch mit großen Zahlen auf dem Rechenschieber zu rechnen. Er gibt dazu Regeln an, wie man zu den einzelnen Koeffizienten der Polynome in der Hunderterdarstellung der jeweiligen Ergebnisse gelangt. Die für den Laien etwas verwirrende Zahlendarstellung als Polynome ist im Bereich der Mathematik üblich und nichts Besonderes. Man beachte auch, dass Herr Schumacher seine Dissertation im Bereich von polynomialen Gleichungen verfasst hat. Daher rührt vermutlich auch die Tatsache, dass Herr Schumacher seine Rechenregeln als sehr einsichtig bzw. einfach empfindet.
Ein gravierender Nachteil des Rechenschiebers ist es, dass er sich nur auf einen Primzahlkörper beschränkt. Zusätzlich ist er auch noch für diesen Primzahlkörper durch die feste Wahl der primitiven Wurzel $w = 2$ eingeschränkt. Wählt man als primitive Wurzel z.B. $w' = 3$, so erfordert dies eine andere Beschriftung des Rechenschiebers. Die Tabelle der diskreten Logarithmen besitzt dann ebenfalls ein anderes Aussehen. Desweiteren müssen die Rechenschieberskalen vollständig neu beschriftet werden, da dort von links nach rechts die Werte $w'^i = 3^i \mod 101$ für $i = 0, \ldots, p-2$ angegeben werden müssen.
Diese Umstände erklären warum der Rechenschieber von Schumacher kein großer Verkaufserfolg war. Ich glaube aber auch nicht, dass jemand bei Faber-Castell mit einem großen Verkaufserfolg gerechnet hat. Fertigungstechnisch dürfte der Rechenschieber keine große Herausforderung gestellt haben, da es bei den Berechnungen ja stets um ganzzahlige Ergebnisse geht und somit keine hohen Anforderungen bzgl. der Genauigkeit der Skalenbeschriftungen vorgegeben waren.
Für weitere Informationen zu Schumachers Rechenschieber verweise ich nochmals auf den Artikel im "Journal of the Oughtred Society" [JezWeiZer2004].

6 Warum der diskrete Logarithmus auf ihr Geld aufpasst

Verlassen wir die Vergangenheit und wenden uns der Gegenwart zu.
Die in den vorhergehenden Kapiteln beschriebenen mathematischen Operationen erscheinen im ersten Moment sehr theoretisch und praxisfern. Aus der Sicht der heutigen Zeit ist dieses jedoch nicht der Fall. Die Berechnungen in Primzahlkörpern und polynomialen Zahlendarstellungen gehören heute zum Standardstoff in Mathematik- und Informatik-Grundvorlesungen, teilweise auch bereits im Mathematik-Abitur. Diese theoretischen Grundlagen finden heutzutage in zahlreichen Produkten des Alltagslebens ihre Anwendung. Beispiele hierfür sind Anwendungen der digitalen Datenübertragung (via Satelliten, aber auch Telefon), digitale Datenträger, dabei speziell für die Fehlererkennung und -korrektur (z.B. auf CDs und DVDs).

Diese Anwendungen nutzen Primkörper, deren Erweiterungen (auf die wir hier nicht eingehen) und ihre mathematischen Eigenschaften aus. Der diskrete Logarithmus spielt dabei keine Rolle.
Es gibt jedoch ein sehr aktuelles Anwendungsgebiet, dass in besonderem Maße auf diskrete Logarithmen aufbaut - die Kryptografie.
Die Sicherheit vieler im Einsatz befindlichen Verschlüsselungsverfahren baut grundlegend darauf auf, dass die Berechnung diskreter Logarithmen in großen Primzahlkörper (d.h. für sehr, sehr große Primzahlen p) extrem schwierig und (bisher) nicht effizient lösbar sind.
Sie vertrauen beim Geldabheben am Bankautomaten ihr Geld somit der Sicherheit des diskreten Logarithmus an! Aber damit Sie nicht aus übereilter Panik ihr Geld sofort vom Konto abheben und zuhause deponieren, werde ich im folgenden Abschnitt erklären, warum ihr Geld auf der Bank besser aufgehoben ist, als bei ihnen zuhause. Dort kann es nämlich relativ schnell gestohlen oder bei einem Brand zerstört werden.

6.1 Das Diskrete-Logarithmus-Problem

Schumacher stattete seinen Rechenschieber mit der Tabelle der diskreten Logarithmen für die Menge der Zahlen $\{1, \ldots, p-1\}$ für die Primzahl $p = 101$ und die primitive Wurzel (das erzeugende Element) $w = 2$ aus. Man beachte, dass für die Zahl 0 kein diskreter Logarithmus existiert (genauso wie bei den reellen Zahlen). Er hat damit eine vollständige Tabelle der Lösung zu folgenden Problem für die Primzahl $p = 101$ und der primitiven Wurzel $w = 2$ angegeben.

6.1.1 Diskretes Logarithmus Problem (DLP)

Gegeben eine Primzahl p. Betrachte die Menge der $\{1, \ldots, p-1\}$ mit der primitive Wurzel w (das erzeugende Element). Für eine beliebige Zahl b, mit $1 \leq b \leq p-1$, berechne die ganze Zahl x, mit $1 \leq x \leq p-1$, so dass gilt

$$w^x \equiv b \mod p.$$

6.2 Kryptoverfahren

Für sehr, sehr große Primzahlen p gibt es bis zum heutigen Tag kein effizientes (d.h. ausreichend schnelles) Rechenverfahren, um dieses Problem zu lösen. Selbst Supercomputer beissen sich an diesem Problem für hinreichend große Primzahlen die Zähne aus.
Während die Berechnung des diskreten Logarithmus extrem schwer sein kann, ist die Umkehroperation, das Exponenzieren einfach und schnell. Einige Abschnitte zuvor hatte ich Ihnen empfohlen $2^{51} \mod 101$ zu berechnen. Dieses kann man mit Hilfe der normalen Potenzregeln bestimmt werden.

$$\begin{aligned} 2^{51} &= 2^{10+10+10+10+10+1} \\ &= 2^{10} * 2^{10} * 2^{10} * 2^{10} * 2^{10} * 2 \\ &= 1024 * 1024 * 1024 * 1024 * 1024 * 2 \end{aligned}$$

Berücksichtigt man das $1024 \equiv 14 \mod 101$ ist (1024 gibt per Division mit 101 den Rest 14), dann ergibt sich

$$\begin{aligned} 2^{51} &\equiv 14 * 14 * 14 * 14 * 14 * 2 \mod 101 \\ &\equiv 99 \mod 101. \end{aligned}$$

Umgekehrt für die Zahl 99 den diskreten Logarithmus 51 zu bestimmen ist wesentlich aufwendiger. Prinzipiell kann man die sogenannte Brute-Force-Methode anwenden, indem man alle Potenzen $2^i \mod 101$ berechnet, bis man das Ergebnis 99 erhält.
Im Mittel benötigt man bei der Brute-Force-Methode $\frac{(p-1)}{2}$ Berechnungen von unterschiedlichen 2^i. Aus diesem Grund müssen für heute angewandte Kryptoverfahren, die auf dem diskreten Logarithmus Problem

beruhen, die verwendeten Primzahlen größer als 2^{1024} oder besser 2^{2048} sein. Für solch große Primzahlen können Sie selbst bei Verwendung eines Supercomputers lange auf das Ergebnis warten.
Tatsächlich gibt es einige Algorithmen, die den diskreten Logarithmus im Mittel schneller berechnen. Beispiele hierfür sind:

- Der Shank's Baby-Step Giant-Step, der die Zeit für die Berechnung größenordnungsmäßig auf $\sqrt{p-1}$ Berechnungen beschränkt, dafür jedoch einen hohen Speicherbedarf für die Rechnungen erfordert.
- Pollands Rho Methode basiert auf dem sogenannten Geburtstags-Paradoxon und verwendet pseudozufällige Exponenten i zur Berechnung der 2^i. Der Algorithmus läuft ähnlich schnell wie der Baby-Step Giant-Step Algorithmus, benötigt jedoch wesentlich weniger Speicherplatz.
- Pohlig-Hellman Algorithmus nutzt das Chinesische Restklassen Theorem, zusammen mit den zuvor genannten Algorithmen.

Für alle genannten Algorithmen gilt jedoch weiterhin, wenn p ausreichend groß ist, dauert die Berechnung des diskreten Logarithmus im Mittel immer noch extrem lange.

6.3 Einwegfunktion

Die Eigenschaft, dass die Potenzierung sehr einfach berechnet werden kann, die Umkehrung, der diskrete Logarithmus, jedoch sehr schwer, bezeichnet man als Einwegfunktion.
Diese Eigenschaft wird in einer Reihe von Verschlüsselungsverfahren verwendet.
Die Verschlüsselung von Daten (Potenzieren) ist schnell berechenbar, das Entschlüsseln jedoch sehr schwer und zeitaufwendig, wenn keine weitere Information (der geheime Schlüssel) bekannt ist.
Beispiele für aktuell verwendete Verschlüsselungsverfahren[3] dieser Art sind:

- Diffie-Hellmann-Key-Exchange Protokoll (DHKE),
- Elgamal Verschlüsselung und der
- Digital Signature Algorithm (DSA), der in Geldautomaten, aber auch im Emailverkehr verwendet wird.

6.4 Elliptische Kurven

Wen die Mathematik in den vorherigen Kapiteln nicht abgeschreckt hat, dem möchte ich zum Abschluss eine noch aktuellere Kryptomethode vorstellen, die ebenfalls auf dem diskreten Logarithmus aufbaut. Es handelt sich dabei um die elliptische Kurven Kryptografie (engl. Elliptic Curve Cyptographie, ECC). Dabei werden wir auf elliptischen Kurven eine Additionsvorschrift definieren, die zwei beliebige Punkte der Kurve so addiert, dass sich ein eindeutiger dritter Punkt auf der Kurve ergibt. Durch mehrfache Anwendung dieser Addition springt man wild auf der Kurve hin und her.

6.4.1 Definition: Elliptische Kurve über den reellen Zahlen

Die elliptische Kurve über den reellen Zahlen $\mathbb{R}$ ist die Menge aller Punktpaare (x, y), die die folgenden Bedingung erfüllt

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

wobei a und b ebenfallse reelle Zahlen sind.
Zusätzlich wird noch in imaginärer Punkt 0 für die Unendlichkeit hinzugefügt. Außerdem muss gelten

$$4 \cdot a^3 + 27 \cdot b^2 \neq 0.$$

(Hinweis: Die seltsam wirkende Zusatzbedingung verhindert, dass sich die elliptische Kurve selber schneidet, bzw. überkreuzt. In diesem Schnittpunkt wäre keine Tangente eindeutig definiert, die für die Rechenoperationen weiter unten jedoch erforderlich sind.)

[3] Ein allgemein verständlicher Artikel über Vershlüsselungsverfahren findet man in [Wob2003].

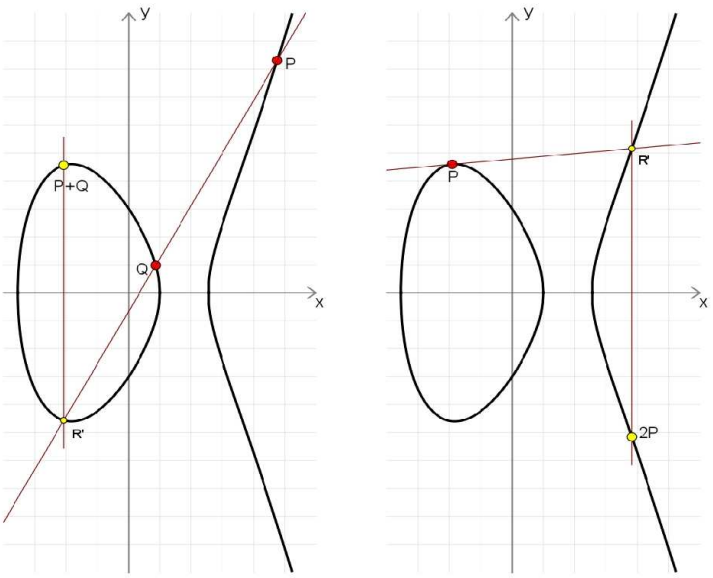

Abbildung 4: Elliptischen Kurve $y^2 = x^3 - 10 \cdot x + 9$: Berechnung von $P + Q$ (links) und $2 \cdot P$ (rechts).

6.4.2 Addition auf elliptischen Kurven

Die Addition $P + Q$ zweier beliebiger Punke $P = (x_p, y_p)$ und $Q = (x_q, y_q)$ auf der Kurve ergibt den Punkt $R = (x_r, y_r)$, indem man folgendermaßen vorgeht:

i. Verbinde die Punkte P und Q durch eine Gerade.

ii. Die Gerade schneidet die Kurve in genau einen weiteren Punkt R'.

iii. Spiegele den Punkt R' an der x-Achse. Der so gefundene Punkt ist der gesuchte Punkt $R = P+Q$ (siehe Abbildung 4, links).

Falls $Q = P$, man addiert also $P + P$, liegt ein Sonderfall vor. In diesem Fall verwendet man die Kurventangente durch den Punkt P, um den Punkt R' zu erhalten. Die Spiegelung an der x-Achse ergibt auch hier das gesuchte Ergbnis für R (siehe Abbildung 4, rechts).
Bei jeder weiteren Addition von P springt man an einen anderen Punkt auf der Kurve. Das Berechnen von $x \cdot P$ für große x ist somit recht einfach. Umgekehrt zu einem gegebenen Punkten R und P herauszufinden, wie groß x sein muss, damit $R = x \cdot P$ gilt, ist wiederum sehr schwer.
Wenn Sie ein wenig mit elliptischen Kurven und den zugehörigen Rechenoperationen experimentieren möchten, können Sie das von Prof. Dr. Stefen Kebekus entwickelte, kostenfreie Tool [Keb2009] vom Internet herunterladen.

6.4.3 Elliptische Kurven über endlichen Zahlenmengen

Im vorherigen Abschnitt haben wir die elliptischen Kurven über den reellen Zahlen beschrieben. Es geht aber noch eine Stufe skuriler. Statt der reellen Zahlen nehmen wir nun wieder die Menge der Zahlen von $\{0, 1, \ldots, p-1\}$ für eine Primzahl p. Auch über dieser Zahlenmenge lassen sich elliptische Kurven mittels der folgenden Gleichung definieren:

$$y^2 \mod p = x^3 + a \cdot x + b \mod p$$

Betrachten wir das Beispiel für $a = 17, b = 8$ und die Primzahl $p = 23$ etwas genauer. Die elliptische Kurve ist durch die Gleichung

$$y^2 \mod 23 = x^3 + 17 \cdot x + 8 \mod 23$$

definiert, in der die Werte von x und y jeweils $\mod$ der Primzahl 23 gerechnet werden.

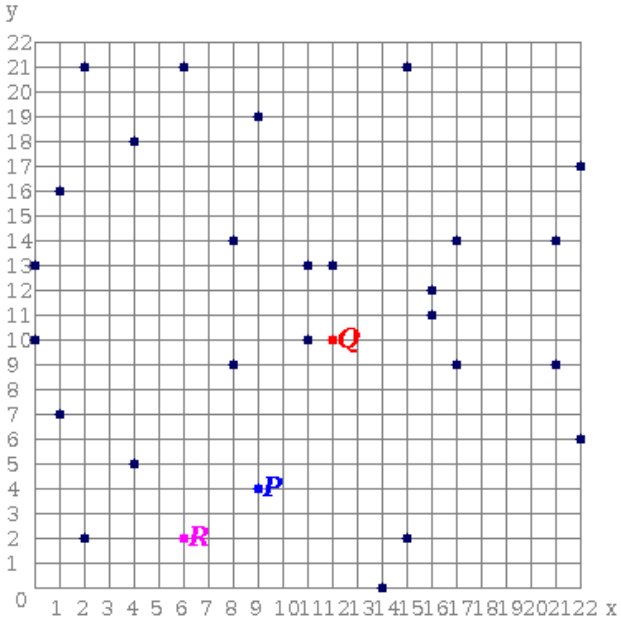

Abbildung 5: Elliptischen Kurve $y^2 \mod 23 = x^3 + 17 \cdot x + 8 \mod 23$ über den Primzahlkörper Z_{23}.

Die 29 Punkte, die die Kurvengleichung erfüllen, sind die in Abbildung 5 markierten Punkte.
Für die Addition zweier Punkte $P = (x_P, y_P)$ und $Q = (x_Q, y_Q)$ ergibt sich das Ergebnis $R = (x_R, y_R)$ folgendermaßen:

$$\begin{aligned} R &= P + Q \text{ mit} \\ m &= \frac{y_P - y_Q}{x_P - x_Q} \mod p \text{ (m ist die “Steigung” der Geraden durch P und Q),} \\ x_R &= s^2 - x_p - x_Q \mod p \text{ und} \\ y_R &= -y_P + m \cdot (x_p - x_R) \mod p. \end{aligned}$$

Für die Addition des Punktes $P = (x_p, y_p)$ (y_p darf nicht 0 sein) zu sich selbst, ergibt sich das Ergebnis $R = (x_R, y_R) = 2 \cdot P$ folgendermaßen:

$$\begin{aligned} R &= 2 \cdot P \text{ mit} \\ m &= \frac{3x_P^2 + a}{2y_P} \mod p, \\ x_R &= m^2 - 2x_p \mod p \text{ und} \\ y_R &= -y_P + m \cdot (x_p - x_R) \mod p. \end{aligned}$$

Abildung 5 zeigt die Punkte $P = (x_P, y_P) = (9, 4)$ und $Q = (x_Q, Y_Q) = (12, 10)$, sowie deren Summe $R = P + Q = (x_R, y_R) = (6, 2)$. Wenn Sie das Ergebnis nicht glauben, rechnen Sie es einfach nach.
Wiederum gilt auch hier, dass bei jeder weiteren Addition von P, man an einen anderen Punkt auf der Kurve springt. Das Berechnen von $x \cdot P$ für große x ist somit recht einfach. Umgekehrt zu einem gegebenen Punkten R und P herauszufinden, wie groß x (der diskrete Logarithmus) sein muss, damit $R = x \cdot P$ gilt, ist wiederum sehr schwer.
Das gilt natürlich nicht für das hier angegebene, kleine Beispiel mit der Primzahl $p = 23$. Für Primzahlen größer als 2^{1024} ist die Berechnung des diskreten Logarithmus jedoch praktisch bis heute nich effizient berechenbar.

6.4.4 Aktuelle Anwendungen für elliptische Kurven

Sie mögen jetzt meinen, dass das zuvor beschriebene nun wirklich nur Theorien ohne praktische Anwendungen sind. Dieses ist jedoch ganz und gar nicht der Fall. Die beschriebenen Methoden für elliptische Kurven haben mittlerweile unbemerkt Einzug in Ihr ganz persönliches Leben genommen.
So stellen heute elliptische Kurven einen sicheren Datentransfer zwischen Geldautomaten und den entsprechenden Servern der zugehörigen Banken sicher.
Eventuell haben Sie auch gerade eine andere Anwendung in Ihrer Tasche dabei, nämlich Ihr Mobiltelefon, dass mittels elliptischer Kurven sich beim Serviceprovider authentifiziert und verschlüsselte Verbindungen aufbaut.
Ein weiteres, möglicherweise ebenfalls in Ihrer Hosen- oder Handtasche befindliche Beispiel, ist Ihr maschinenlesbarer Reisepass oder Personalausweis, die von der Bundesregierung aktuell herausgegeben werden. Auch hier kommen elliptische Kurven zum Einsatz, wie man im technischen Report [Bun2013] des Bundesamtes für Sicherheit in der Informationstechnik nachlesen kann.
Meine Eingangsaussage, dass der diskrete Logarithmus auf Ihr Geld aufpasst, muss ich somit sogar noch dahingehend erweitern, dass der diskrete Logarithmus mittels elliptischer Kurven dem deutschen Staat hilft, auf Sie aufzupassen.

Literatur

[Bun2013] Bundesamt für Sicherheit in der Informationstechnik. eCard-Projekte der Bundesregierung. Teil 2 - Hoheitliche Ausweisdokumente. Technischer Bericht Technische Richtlinie TR-03116-2, 21.03.2013.

[Fab1908p] A. W. Faber. (?). DRGM 344576, 1908.

[JezWeiZer2004] Dieter von Jezierski, Detlef Zerfowski und Paul Weinmann. A. W. Faber Model 366 - System Schumacher. A Very Unusual Slide Rule. *Journal of the Oughtred Society*, 13(2), Seiten 10–17, 2004.

[Keb2009] Stefen Kebekus. `http://home.mathematik.uni-freiburg.de/kebekus/software/ellipticcurve-de.html` Stand: 03.05.2012, 2009.

[ParPel2010] Christof Paar und Jan Pelzl. *Understanding Cryptography. A Textbook for Students and Practitioners.* Springer, Heidelberg, Drodrecht, London, New York, 2010.

[Sch1884] Joh. Schumacher. *Zur Theorie der biquadratischen Gleichungen.* Phd thesis, Universität Erlangen, 1884.

[Sch1909] Joh. Schumacher. *Ein Rechenschieber mit Teilung in gleiche Intervalle auf Grundlage der zahlentheoretischen Indizes. (D.R.G.M. Nr. 344576). Für den Unterricht konstruiert.* J. Lindauersche Buchhandlung, Schöpping, München, 1909.

[Wie1909-1] Heinrich Wieleitner. Rezension. *Zeitschrift für mathematischen und naturwissenschaftlichen Unterricht*, (40), 1909.

[Wob2003] Reinhard Wobst. Harte Nüsse. Verschlüsselungsverfahren und ihre Anwendungen. *c't*, (17), Seite 200ff, August 2003.