Elliptische Kurven in Theorie und Anwendung

Johann Wiesenbauer, TU Wien

Zusammenfassung

Das Studium der Elliptischen Kurven, d.h. der algebraischen Kurven vom Geschlecht 1, schließt in natürlicher Weise an die in der Schule seit jeher vielbetriebenen Untersuchungen von Geraden und Kegelschnitten an, welche zu den Kurven vom Geschlecht 0 gehören. So wie für diese existieren auch für Elliptische Kurven eine Fülle von Anwendungen, z.B. bei der Auflösung Diophantischer Gleichungen, bei Primzahltests und Faktorisierungsverfahren für ganze Zahlen, und neuerdings auch in der Kryptographie im Zusammenhang mit wichtigen asymmetrischen Chiffrierverfahren. In der Arbeit wird versucht, an Hand einiger konkret mit Hilfe von Derive 5 durchgerechneter Beispiele einen kleinen Einblick in diese Möglichkeiten zu geben.

„It is possible to write endlessly on elliptic curves...
This is not a threat."

Serge Lang (in [4])

Obiges Eingangszitat hat vor allem eine apologetische Funktion, indem es deutlich machen soll, dass in Hinblick auf das gestellte Thema eine auch nur annähernde Vollständigkeit – und das selbst in ganz grundsätzlichen Fragen – keinesfalls möglich ist, ganz abgesehen davon, dass man dazu tief in der Schulmathematik eher fernliegende Teilgebiete der Mathematik, wie z.B. der Funktionentheorie oder der Algebraischen Geometrie eindringen müßte. Ich habe daher versucht, aus der Not eine Tugend zu machen und im folgenden exemplarisch einige, wie ich meine, besonders interessante Problemstellungen ausgewählt, bei deren Behandlung Elliptische Kurven eine wichtige Rolle spielen und wo trotzdem nicht allzuviel an „Theorie" benötigt wird. Viele der vorgestellten Anwendungen sind dabei noch keine zwanzig Jahre alt und belegen damit ganz nebenbei recht eindrucksvoll, dass auch heute noch – und sogar mehr als je, wenn man sich die riesige Menge an Publikationen ansieht - die Mathematik im ständigen Wachstum begriffen ist.

1. Was ist eine elliptische Kurve?

Dass in einer schulgerechten Darstellung an vielen Stellen Kompromisse eingegangen werden müssen, wird bereits zu Beginn beim Versuch einer Definition der elliptischen Kurve sehr deutlich. Eine mögliche Definition könnte z.B. so aussehen: Eine elliptische Kurve über einen Körper K ist eine eindimensionale projektive Varietät vom Geschlecht 1 über K mit mindestens einem K-rationalen Punkt. Hier kommen aber doch eine ganze Reihe von Begriffen vor, welche einer Erklärung bedürfen.

Zum Glück ist aber ohne allzu große Einschränkung der Allgemeinheit für unsere Zwecke eine sehr viel einfachere Definition einer elliptischen Kurve über einem Körper K bereits ausreichend, nämlich als die Menge aller Lösungen $(x,y) \in K \times K$ einer Gleichung der Form

$$y^2 = x^3 + ax + b \quad (a,b \in K)$$

ergänzt um den sog. „unendlich fernen" Punkt O. Dabei setzt man noch voraus, dass diese Gleichung überhaupt eine Lösung besitzt, d.h., dass es in obiger Sprechweise „mindestens einen K-rationalen Punkt gibt", und das rechtsstehende Polynom $f(x) = x^3 + ax + b$ keine mehrfachen Nullstellen besitzt, was man auch so ausdrücken kann, dass $f(x)$ und $f'(x)$ niemals gleichzeitig verschwinden. Die letztere Bedingung gilt dabei sogar verschärft nicht nur in K, sondern sogar im sog. algebraischen $\overline{K}$ von K. (Der algebraischen Abschluss $\overline{K}$ von K ist dabei in gewisser Hinsicht der „kleinste" Erweiterungskörper von K, in dem jedes Polynom von K[x] vollständig in Linearfaktoren zerfällt. Er spielt somit für K dieselbe Rolle, wie der Körper **C** der komplexen Zahlen für den Körper **R** der reellen Zahlen.)

Um die Bedeutung dieser auf den ersten Blick seltsam anmutenden Bedingungen für eine elliptische Kurve zu erhellen, möchte ich doch zumindestens versuchen den Zusammenhang zu obiger allgemeiner Definition herzustellen, da hierbei auch sonst einige wichtige Aspekte ins Spiel kommen.

Zunächst einmal bezog sich unsere einfachere Definition auf eine elliptische Kurve in sog. „affiner Darstellung", welche der üblichen Darstellung von implizit gegebenen Funktionen entspricht, die uns von den Kegelschnitten her schon vertraut ist. Um auf die entsprechende projektive Darstellung, welche hier die Form

$$Y^2Z = X^3 + aXZ^2 + BZ^3 \quad (a,b \in K)$$

hat, zu kommen, müssen wir nur in der affinen Gleichung die Substitution x = X/Z und y = Y/Z vornehmen und sie anschließend mit Z^3 multiplizieren. (Zurück zur affinen Darstellung geht's dann einfacher indem man einfach X = x, Y = y, Z = 1 substituiert.)

Auch in der projektiven Darstellung werden wieder alle Lösungen $(X,Y,Z) \in K^3$ dieser Gleichung betrachtet, die triviale Lösung (0,0,0) jedoch explizit ausgenommen. Dabei werden aber zwei Punkte (X_1,Y_1,Z_1) und (X_2,Y_2,Z_2) als gleich angesehen, falls es ein $t \in K\backslash\{0\}$ gibt, sodass gilt $(X_1,Y_1,Z_1) = t(X_2,Y_2,Z_2)$. Nach dieser Identifikation entsprechen sich die Punkte der affinen und projektiven Darstellung der elliptischen Kurve E über K umkehrbar eindeutig bei der bijektiven Zuordnung $(x,y) \leftrightarrow (x,y,1)$ $(x,y \in K)$ ergänzt durch $O \leftrightarrow (0,1,0)$.

Scheinbar ist also kein Unterschied zwischen diesen beiden Darstellungen? Weit gefehlt: Der Punkt O, der in der affinen Darstellung ein „Außenseiterdasein" geführt hatte und dessen Vorhandensein wir bisher eigentlich noch gar nicht richtig begründet hatten, ist in der projektiven Darstellung nun vollkommen „integriert" und wir können insbesondere mit ihm rechnen, wie mit jedem anderen Punkt auch. Ein weiterer wichtiger Vorteil ist, dass das Rechnen mit „Brüchen" in der projektiven Darstellung generell leicht vermieden werden kann, wenn man dies wünscht. Tatsächlich ist ja z.B. der Punkt (2/3, 1/2, 3) über dem Körper **Q** der rationalen Zahlen nach obigem identisch mit dem Punkt (4,3,18), da letzterer durch Multiplikation mit dem gemeinsamen Nenner t=6 aus ersteren hervorgeht.

Da ferner in der projektiven Darstellung die Elliptische Kurve aus den Nullstellen eines Polynoms $F(X,Y,Z) \in K[X,Y,Z]$, nämlich hier

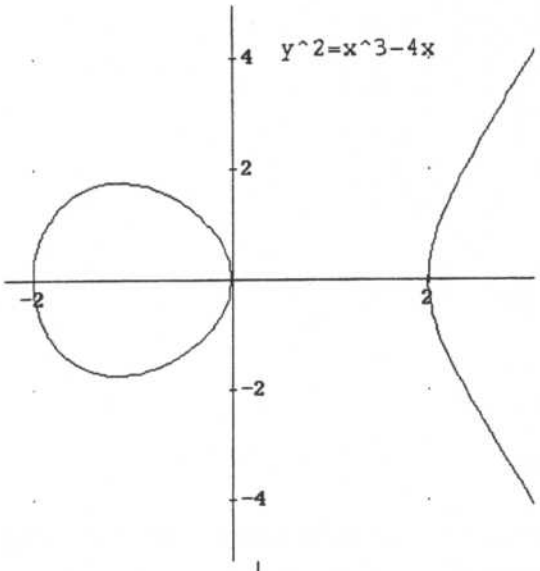
$$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - BZ^3$$

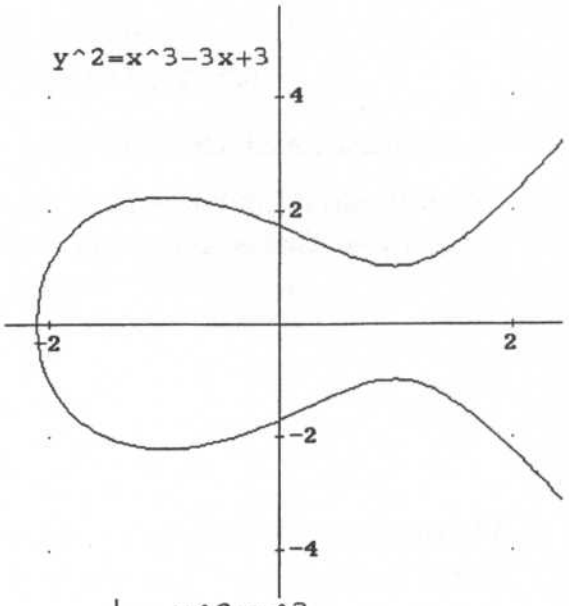
erhalten wird und wir bei der Wahl der Koordinaten gemäß obiger Identifikation gewissermaßen nur einen „Freiheitsgrad" mehr haben, liegt tatsächlich eine sog. projektiven Varietät der Dimension 1 vor. Zur Berechnung des Geschlechts g einer projektiven Varietät, d.h. der Menge der Nullstellen einer allgemeinen Polynoms $F(X,Y,Z) \in K[X,Y,Z]$, bedient man sich am besten der Formel von Plücker, nämlich

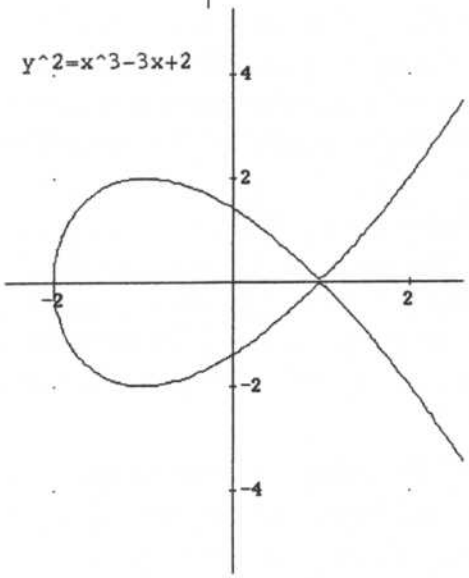
$$g = \frac{(n-1)(n-2)}{2} - s$$

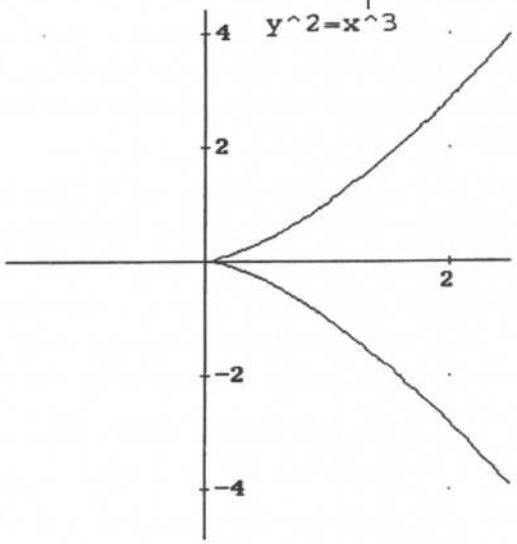
wobei hier n den Grad von F(X,Y,Z) und s die Anzahl der Singularitäten von F(X,Y,Z) bezeichnet, d.h. diejenigen Punkte der Kurve, in denen sämtliche partiellen Ableitungen verschwinden.

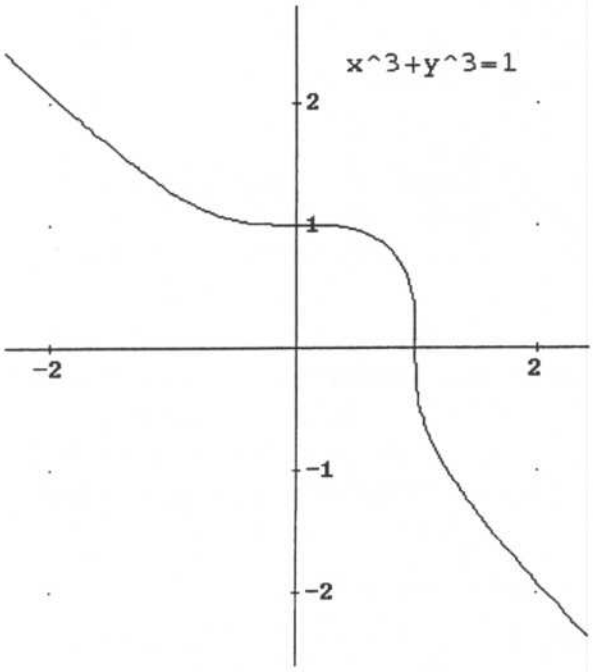
Diese Formel für das Geschlecht gilt in dieser Form jedoch nur, wenn die Kurve keine anderen Singularitäten als gewöhnliche Doppelpunkte und Spitzen hat. Singularitäten mit einer Vielfachheit r>2, in denen es anschaulich gesprochen r Tangenten gibt, muss man in obiger Formel als r(r-1)/2 Doppelpunkte „in Rechnung stellen". Nachfolgend sind einige einfache Beispiele von algebraischen Kurven mit und ohne Singularitäten zusammengestellt.

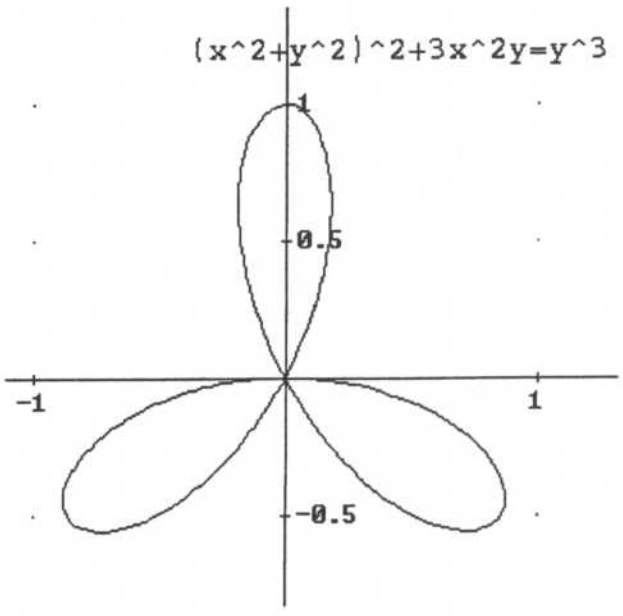

y^2=x^3-4x
4
2
-2
2
-2
-4


y^2=x^3-3x+3
4
2
-2
2
-2
-4


y^2=x^3-3x+2
4
2
-2
2
-2
-4


y^2=x^3
4
2
2
-2
-4


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


(x^2+y^2)^2+3x^2y=y^3
1
0.5
-1
1
-0.5

Rein rechnerisch sind Singularitäten die Lösungen des polynomialen Gleichungssystems

$$F(X,Y,Z) = F_X(X,Y,Z) = F_Y(X,Y,Z) = F_Z(X,Y,Z) = 0$$

im algebraischen Abschluß $\overline{K}$ von K.

Versucht man damit konkret die Singularitäten für $F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - BZ^3$ zu berechnen, so kommt man auf die Gleichungen

$$\begin{aligned} Y^2Z - X^3 - aXZ^2 - BZ^3 &= 0 \\ -3X^2 - aZ^2 &= 0 \\ 2YZ^2 &= 0 \\ Y^2 - 2aX - 3BZ^2 &= 0 \end{aligned}$$

Wegen der letzten Gleichung sieht man sofort, dass (0,1,0) niemals singulär ist. Für einen Körper K mit char(K)≠2, in dem also 2y=0 nur für y=0 gilt, ist aber auch kein Punkt (x,y,1) singulär, da sonst aus obigen Gleichungen f(x)=f'(x)=0 für das Polynom $f(x)=x^3+ax+b$ in der affinen Darstellung folgen würde, d.h. x wäre entgegen der Voraussetzung eine doppelte Nullstelle von f(x). Mit n=3 und s=0 erhält man somit aus obiger Formel für das Geschlecht g tatsächlich den Wert 1.

Man kann nun zeigen, dass außer für Körper K mit char(K) = 2 oder char(K) = 3 (für die also gilt 1+1=0 bzw. 1+1+1=0), auch umgekehrte jede elliptische Kurve im Sinne der allgemeinen Definition durch eine sog. „birationale Transformation" – dies ist eine umkehrbare Koordinatentransformation, bei der die die Transformationsgleichungen durch rationale Funktionen über K beschrieben werden – auf die von uns angegeben Form gebracht werden kann, welche auch (kurze) Weierstraßform genannt wird.

Für die zwei genannten Ausnahmefälle char(K) = 2,3 sind die Dinge nur leicht komplizierter: Ist char(K)=3, so gilt wieder $y^2 = f(x)$, wobei jetzt das rechtsstehende Polynom $f(x)\in K[x]$ die etwas allgemeinere Form $f(x)=x^3+ax^2+bx+c$ hat, während im Fall char(K)=2 die Gleichung der elliptischen Kurve eine der beiden Formen

$$\left.\begin{matrix} y^2+xy \\ y^2+cy \end{matrix}\right\} = x^3+ax+b$$

gebracht werden kann, wobei der erstgenannte Typ für Zwecke der Kryptographie große Bedeutung hat. (Der zweite Typ führt auf sog. supersinguläre Kurven, welche in Hinblick auf gewisse Kryptoattacken eine deutlich bessere Angriffsfläche bieten und daher in diesem Zusammenhang tunlichst vermieden werden sollten!)

Wie inzwischen klar geworden sein dürfte, kann man von einer beliebigen algebraischen Kurve oft gar nicht so einfach sagen, ob es sich dabei um eine elliptische Kurve handelt oder nicht. Als erstes wird man dazu ihr Geschlecht bestimmen. Von den obigen 6 Kurven haben die ersten fünf den Grad 3 und daher nach der Plückerschen Formel genau dann das Geschlecht 1, wenn sie nichtsingulär, d.h. frei von Singularitäten sind. Dies trifft, wie man sofort nachrechnet, für die Kurven

$$y^2 = x^3 - 4x, \quad y^2 = x^3 - 3x + 3 \quad \text{und} \quad x^3 + y^3 = 1$$

zu, welche daher für K=**R** tatsächlich elliptische Kurven sind, da diese Gleichungen dann offensichtlich auch Lösungen in K besitzen. Insbesondere müßte sich also die letzte Kurve, die noch nicht in Weierstraßform gegeben ist, nach dem oben Gesagten durch eine birationale Transformation auf eine solche bringen lassen. Tatsächlich ist dies der Fall, wie die folgende Rechnung in Derive 5 beweist,

$$x^3 \cdot \text{SUBST}\left[x^3 + y^3 - 1,\ [x,\ y],\ \left[\frac{y + 36}{6 \cdot x},\ \frac{36 - y}{6 \cdot x}\right]\right] = -x^3 + y^2 + 432$$

d.h. die Kurven $x^3 + y^3 = 1$ und $y^2 = x^3 - 432$ sind „birational äquivalent".

Ist am Ende auch die letzte Kurve $(x^2 + y^2)^2 + 3x^2y = y^3$, das berühmte „3-blättrige Kartesische Kleeblatt" eine elliptische Kurve? Dazu müssen wir die Vielfachheit der einzigen Singularität im Punkt (0,0) bestimmen, welche die Mindestvielfachheit ist, mit der eine beliebige Gerade y=kx durch (0,0) die Kurve im Punkt (0,0) schneidet. Wegen

$$h(x,\ y) := (x^2 + y^2)^2 + 3 \cdot x^2 \cdot y - y^3$$

$$h(x,\ k \cdot x) = x^4 \cdot (k^2 + 1)^2 + k \cdot x^3 \cdot (3 - k^2)$$

beträgt diese offenbar 3, d.h., es gibt drei Tangenten in (0,0), nämlich mit den Steigungen k=0 und $k = \pm\sqrt{3}$, was man hier auch noch „mit freiem Auge" hätte sehen können. Diese Singularität ist daher so wie 3 (= 3*2/2) gewöhnliche Doppelpunkte zu bewerten. Einsetzen der Werte n=4 und s=3 in die Plückersche Formel ergibt dann, dass die vorliegende Kurve Geschlecht 0 hat, also keine elliptische Kurve ist. Insbesondere kann man daraus folgern, dass sie so wie alle Kurven vom Geschlecht 0, zu denen ja auch die Geraden und Kegelschnitte zählen, eine parametrische Darstellung mit Hilfe von rationalen Funktionen besitzen muss. Es ist recht lehrreich, wie man auf eine solche kommen kann: Man betrachtet dazu wieder die Geraden y=kx durch (0,0) und bestimmt einfach den eindeutigen Schnittpunkt $\neq (0,0)$ mit der Kurve, der sich zu

$$x = \frac{k(k^2 - 3)}{(k^2 + 1)^2}, \quad y = \frac{k^2(k^2 - 3)}{(k^2 + 1)^2}$$

ergibt, was damit die Parameterdarstellung angibt. Insbesondere sieht man so sofort, dass es unendlich viele rationale Punkte auf der Kurve gibt.

Allgemeiner kann man mit der gleichen Beweisidee für Kurven vom Geschlecht 0 über $\mathbf{Q}$ zeigen (und der Leser möge sich dies z.B. für Kreise $x^2 + y^2 = r^2$ mit $r \in \mathbf{Q}$ selbst überlegen!), dass auf ihnen entweder keine oder unendliche viele rationale Punkte liegen, d.h. die Frage nach den rationalen Punkten ist für sie in gewisser Weise trivial. Für Kurven vom Geschlecht $g \geq 2$ über $\mathbf{Q}$ konnte dagegen Faltings 1983 eine alte Vermutung von Mordell zeigen, dass nämlich auf ihnen stets höchstens endlich viele rationale Punkte liegen. Es bleiben also noch die elliptischen Kurven über $\mathbf{Q}$, für welche genau diese Frage nach der Anzahl der rationalen Punkte zu den knifflichsten überhaupt gehört, über die schon ganze Bücher geschrieben wurden (siehe z.B. [8]). Wir werden in Kürze noch einmal darauf zurückkommen.

2. Ein altes Problem und neue Einsichten

Ein Problem, welches schon von den alten Griechen studiert wurde und welches, wie wir gleich sehen werden, eng mit gewissen elliptischen Kurven zusammenhängt, ist die Bestimmung der sog. kongruenten Zahlen. Eine quadratfreie ganze Zahl d>0 heißt dabei kongruent, wenn sie sich als Flächeninhalt eines rechtwinkeligen Dreiecks mit rationalen Seiten a,b,c darstellen läßt. (a,b bezeichne dabei wie üblich die Katheten und c die Hypothenuse des Dreiecks.) Wie man sofort sieht, ist daher z.B. d=6 eine kongruente Zahl, denn sie ist der Flächeninhalt des klassischen rechtwinkeligen Dreiecks mit den (hier sogar ganzzahligen!) Seiten 3,4 und 5. Etwas weniger trivial ist bereits die Auffindung eines solchen Dreiecks mit Flächeninhalt 5. (Wir werden ein solches weiter unten berechnen, aber der Leser möge in der Zwischenzeit sich selbst daran versuchen!) Für gewisse Zahlen d gibt

es sogar überhaupt kein derartiges Dreieck, d.h. sie sind nicht kongruent. So konnte dies z.B. schon Fermat um 1650 für d=1 zeigen, indem er die Diophantische Gleichung $x^4 + y^4 = z^2$ untersuchte. Auch für d=2 und d=3 existieren keine derartigen Lösungen.

Wie nun folgende Rechnung mit Derive zeigt, liefert jedes rechtwinkelige Dreieck mit den Seiten a,b,c sofort eine rationale Lösung (x,y) mit y≠0 der elliptischen Kurve $y^2 = x^3 - d^2x$:

$$\left[x := \frac{a\cdot(a - \sqrt{(a^2 + b^2)})}{2},\ y := \frac{a^2\cdot(\sqrt{(a^2 + b^2)} - a)}{2},\ d := \frac{a\cdot b}{2}\right]$$

$$y^2 - x^3 + d^2\cdot x = 0$$

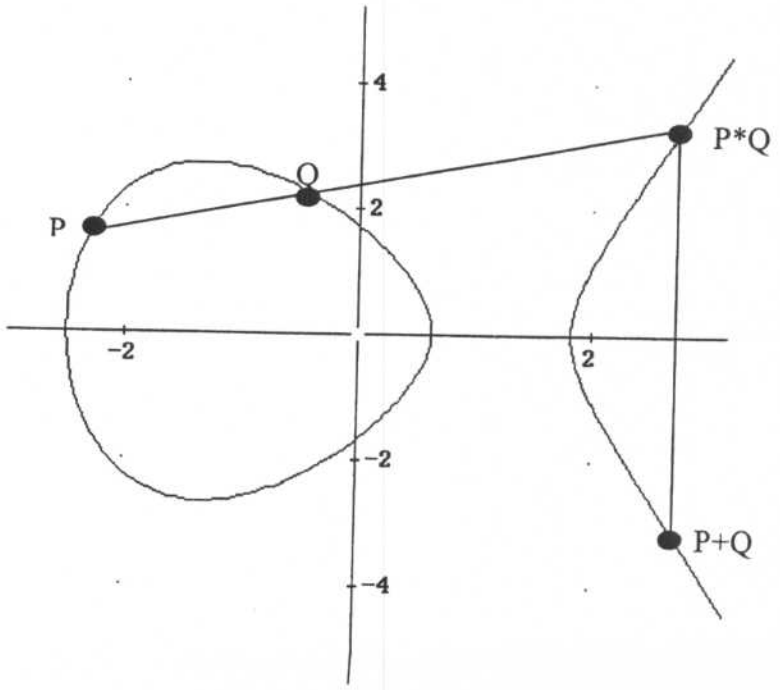
Es gilt aber auch die Umkehrung, d.h. ist (x,y) mit y≠0 ein rationaler Punkt der elliptischen Kurve $y^2 = x^3 - d^2x$, so erhält man mit nachfolgenden Definitionen ein rechtwinkeliges Dreieck mit rationalen Seiten a,b,c und Flächeninhalt d:

$$\left[a := \left|\frac{x^2 - d^2}{y}\right|,\ b := \left|\frac{2\cdot x\cdot d}{y}\right|,\ c := \left|\frac{x^2 + d^2}{y}\right|,\ y := \pm\sqrt{(x^3 - d^2\cdot x)}\right]$$

$$a^2 + b^2 - c^2 = 0$$

$$a\cdot b = 2\cdot|d|$$

Was aber ist durch diese Transformation auf ein Problem über elliptische Kurven gewonnen? Wie wir gleich sehen werden eine ganze Menge! In erster Linie liegt dies an der wunderbaren Eigenschaft der elliptischen Kurven, dass man auf der Menge ihrer Punkte eine Addition einführen kann, welche sie zu einer abelschen Gruppe werden läßt. Die Summe P+Q zweier Punkte P und Q einer elliptische Kurven über **R** erhält man dabei im allgemeinen Fall so, dass man die Sekante durch P und Q legt (bzw. die Tangente an P, falls P und Q zusammenfallen!) und den Schnittpunkte P*Q an der x-Achse spiegelt, so wie unten dargestellt.



Sind $P=(x_1,y_1)$ und $Q=(x_2,y_2)$ die Koordinatendarstellungen der beiden Punkte, so ergeben sich zunächst die Steigung k der Sekante (bzw. Tangente für P=Q) zu

$$k=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & \text{falls } x_1\neq x_2\\ \dfrac{3x_1^2+a}{2y_1}, & \text{falls } x_1=x_2, y_1\neq 0\end{cases}$$

und daraus durch Einsetzen von $y=k(x-x_1)+y_1$ in die Gleichung $y^2=x^3+ax+b$ der elliptischen Kurve nach leichter Rechnung die Gleichungen

$$x_3=k^2-x_1-x_2,\quad y_3=-y_1+k(x_1-x_3)$$

für die Koordinaten des Punkts $P+Q=(x_3,y_3)$.

Allerdings haben wir bisher den Fall noch nicht berücksichtigt, dass $x_1=x_2$, aber $y_1\neq y_2$. In diesem Fall gilt dann $y_2=-y_1$, d.h. P und Q liegen spiegelbildlich zur x-Achse und wir definieren hier P+Q=O. Schließlich soll noch gelten P+O=O+P=P, d.h. O spielt die Rolle des neutralen Elements für unsere Addition.

Diese Punktaddition kann man nun in der genau gleichen Weise, aber eben dann ohne die geometrische Interpretation, auch für einen beliebigen Körper K durch obige Gleichungen definieren und erhält so, wie man beweisen kann, in jedem Falle eine abelsche Gruppe, welche wir im folgenden mit E(K) (oder auch nur E) bezeichnen.

Was kann man aus algebraischer Sicht über die Struktur dieser abelschen Gruppe aussagen? Betrachten wir zunächst den wichtigen Spezialfall K=**Q**. Ein klassisches Resultat in dieser Richtung ist dann der Satz von Mordell aus dem Jahre 1923, welcher aussagt, dass E(**Q**) stets endlich erzeugt ist, d.h. es gibt eine endliche Teilmenge $B=\{P_1,...,P_n\}$ von E(**Q**), welche auch Basis von E(**Q**) genannt wird, sodass jeder Punkt $P\in E(\mathbf{Q})$ eine eindeutige Summendarstellung

$$P=k_1P_1+...+k_nP_n\quad (0\le k_i<\mathrm{ord}(P_i))$$

besitzt. Hierbei ist für einen Punkt R seine Ordnung ord(R) definiert als die kleinste unter allen ganzen Zahlen $k>0$ mit kR=O, falls so ein k überhaupt existiert, ansonsten wird $\mathrm{ord}(R)=\infty$ gesetzt. Die Anzahl $r\ge 0$ aller Basispunkte von unendlicher Ordnung ist übrigens eine wichtige Invariante der Gruppe E(**Q**), welche in gewisser Weise ihre „Größe" misst und als ihr Rang bezeichnet wird. Obwohl diese Kennzahl für konkrete elliptische Kurven über **Q** in der Regel ziemlich klein und häufig sogar 0 ist, wird doch vermutet, dass sie insgesamt gesehen unbeschränkt groß sein kann.

Sehr weitgehende Aussagen kann man auch über dies sog. Torsionsgruppe $E(\mathbf{Q})_{tors}$ machen, welche aus allen Punkten P besteht, d.h. für welche gilt $\mathrm{ord}(P)<\infty$ und die auch Torsionspunkte genannt werden. Z.B. gilt nach einem bekannten Satz von Nagell-Lutz aus dem Jahr 1937, dass aus $(x,y)\in E(\mathbf{Q})_{tors}$ stets $x,y\in\mathbf{Z}$, sowie y=0 oder $y^2\mid 4a^3+27b^2$ folgt, was die praktische Berechnung der Torsionspunkte sehr einfach macht. Es war ferner auch schon lange bekannt, dass man höchstens zwei Torsionspunkte braucht, um $E(\mathbf{Q})_{tors}$ zu erzeugen. 1977 gelang es B. Mazur darüber hinaus in einem tiefliegenden Satz eine genaue Liste aller 15 möglichen Fälle für die Struktur von $E(\mathbf{Q})_{tors}$ angeben, aus welchem insbe-

sondere folgt, dass es höchstens 16 Torsionspunkte geben kann und diese nur die Ordnungen 1,2,..,10 und 12 haben können.

Speziell für die elliptischen Kurven $y^2 = x^3 - d^2x$, welche wir oben betrachtet hatten, stellt man übrigens unschwer fest, dass sie genau die vier Torsionspunkte O, (0,0), (d,0), (-d,0) besitzt. Dies sind andererseits genau jene Punkte, denen wir bei obiger Zuordnung keine rationale Lösung des Gleichungssystems

$$a^2 + b^2 = c^2 \ \wedge ab = 2d \qquad (*)$$

zuordnen können. Jeder weitere rationale Punkt von $E(\mathbf{Q})$ liegt aber dann nicht in $E(\mathbf{Q})_{tors}$, womit er zusammen mit seinen Vielfachen automatisch unendliche viele rationale Punkte von $E(\mathbf{Q})$ und damit unendliche viele rationale Lösungen von (*) „produziert". Dies können wir aber nach obigem auch kürzer so ausdrücken, dass (*) genau dann in rationalen Zahlen lösbar ist, wenn die zugehörige elliptische Kurve $E(\mathbf{Q})$ mindestens den Rang 1 hat.

Es ist nun interessant festzustellen, dass die Überprüfung dieser Bedingung, welche im allgemeinen doch einige Schwierigkeiten macht, ganz einfach wäre, würde eine berühmte Vermutung von Birch und Swinnerton-Dyer gelten, auf deren Beweis das Clay Mathematics Institute immerhin ein Preisgeld von $ 1,000,000 ausgesetzt hat, was ihre Wichtigkeit doch eindrucksvoll unterstreicht. Leider erfordert ihre genaue Formulierung einiges an Voraussetzungen aus der Funktionentheorie, weshalb ich mich hier wiederum mit nachfolgenden Andeutungen begnügen muss.

Man betrachtet dazu die jeder elliptischen Kurve E über Q in „kanonischer Weise" zugeordnete L-Reihe L(E,s), von der man allgemein zeigen kann, dass sie für s>3/2 konvergiert. Betrachtet man dazu ihre sog. analytische Fortsetzung auf die ganze Gaußsche Zahlenebene, deren Existenz hier beweisbar ist, so besagt die angesprochene Vermutung, dass der Rang r von E genau mit der Vielfachheit der Nullstelle von L(E,s) für s=1 übereinstimmt. Unter der Annahme der Richtigkeit dieser Vermutung wäre also (*) in rationalen Zahlen genau dann lösbar, wenn für die zugeordnete elliptische Kurve E gilt L(E,1)=0. Leider konnte bislang allgemein nur die Notwendigkeit dieser Bedingung für die Lösbarkeit gezeigt werden (Coates and Wiles, 1977). Was die Umkehrung betrifft, konnten aber Gross und Zagier 1984 immerhin zeigen, dass sie gilt, falls L(E,s) für s=1 eine einfache Nullstelle besitzt.

Wir haben bisher nur den klassischen Fall K=**Q** betrachtet, speziell in Hinblick auf Anwendungen in der Kryptographie aber noch sehr wichtig ist der Fall $K=\mathbf{F}_q$, d.h. wo K ein endlicher Körper mit q Elementen ist, wobei $q = p^m$ eine Primzahlpotenz sein muss. Auch hier gelten nun ähnliche Sätze für die elliptische Kurve $E(\mathbf{F}_q)$ wie vorher für K=**Q**, aber die Tatsache, dass sie endlich ist, macht doch einiges einfacher. So kann man relativ leicht zeigen, dass $E(\mathbf{F}_q)$ stets entweder zyklisch ist oder eine höchstens zweielementige Basis {A,B} besitzt. In letzterem Fall dürfen wir auch noch $ord(A)|ord(B)$, sowie $ord(A)|q-1$ voraussetzen. Sehr wichtig ist auch noch der Satz von Hasse, welcher aussagt, dass $\#\, E(\mathbf{F}_q)$ nicht allzu sehr von q+1 nach oben oder unten abweicht, genauer um höchstens $2\sqrt{q}$.

Nach soviel „Theorie" wollen wir aber nun endlich zum „praktischen Teil" übergehen und einige Beispiele rechnen. Zu diesem Zweck habe ich nachfolgend einige nützliche Derive-Routinen angegeben, wobei ich mich der Einfachheit halber auf die für uns wichtigsten Fälle K=**Q** bzw. $K=\mathbf{F}_p$ für eine Primzahl p beschränkt habe. (Nur in letzterem Fall ist dabei der Eingabeparameter p in nachfolgenden Routinen explizit anzugeben!)

Die erste Routine überprüft, ob die vorgegebene elliptische Kurve $y^2 = x^3 + ax + b$ über dem betrachteten Körper K wirklich nichtsingulär ist, d.h. ob $f(x)=x^3+ax+b$ und $f'(x) = 3x^2 + b$

keine gemeinsame Nullstelle im algebraischen Abschluß $\overline{K}$ haben. Es wird dazu die sog. Diskriminante $4a^3+27b^2$ des Polynoms f(x) verwendet, welche uns bereits im Zusammenhang mit dem Satz von Nagell-Lutz begegnet ist.

```
nonsingular(a, b, p := 0) := SOLVE(MOD(4·a^3 + 27·b^2, p) ≠ 0)

nonsingular(1, 1, 5) = true
```

Wer sich darüber hinaus für den Ausdruck $4a^3+27b^2$ interessiert, dem sei noch verraten, dass er sich rein rechnerisch auch als sog. Resultante von f(x) und f'(x)

$$\text{DET}\begin{bmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{bmatrix} = 4\cdot a^3 + 27\cdot b^2$$

ergibt, was nichts anderes bedeutet, als dass er genau dann verschwindet, wenn die Polynome f(x),xf(x),f'(x),xf'(x), x^2f'(x) in K[x], welchen in obiger Matrix genau die Zeilenvektoren entsprechen, über K linear abhängig sind. Genau in diesem Fall hat aber kgV(f(x),f'(x)) einen kleineren Grad als f(x)f'(x), d.h. f(x) und f'(x) sind dann in K[x] nicht teilerfremd.

Nun zur Abwechslung ein etwas aufwändigeres Programm, das zur Berechnung von Punkten auf einer elliptischen Kurve dient. Im Falle K=**Q**, d.h. für p=0, ist dabei h unbedingt miteinzugeben und bedeutet dann die sog. max. „Höhe", d.h. ein Suchlimit für die Beträge von Zählern und Nennern der jeweiligen x-Koordinaten. Wird dagegen mod p gerechnet, so bedeutet h einfach eine obere Schranke für die Anzahl der zu suchenden Punkte. Hier sind insbesondere die Werte h=1 und h=∞ sinnvoll, wobei dann nur ein Punkt bzw. alle Punkte der Kurve ausgegeben werden.

```
points(a, b, p := 0, h := ∞, u_ := 0, v_, w_ := {}) :=
  If p = 0
     Loop
       v_ := 1
       Loop
         If RATIONAL?(√((u_/v_^2)^3 + a·(u_/v_^2) + b))
            w_ := ADJOIN([u_/v_^2, ± √((u_/v_^2)^3 + a·(u_/v_^2) + b)], w_)
         If RATIONAL?(√(- (u_/v_^2)^3 - a·(u_/v_^2) + b))
            w_ := ADJOIN([- u_/v_^2, ± √(- (u_/v_^2)^3 - a·(u_/v_^2) + b)], w_)
         v_ :+ 1
         If v_^2 > h exit
       u_ :+ 1
       If u_ > h
          RETURN w_
     Loop
       v_ := SQUARE_ROOT(u_^3 + a·u_ + b, p)
       If NUMBER?(v_)
          Prog
            w_ := ADJOIN([u_, v_], w_)
            h :- 1
            If p > 2 ∧ v_ > 0 ∧ h > 0
               [w_ := ADJOIN([u_, p - v_], w_), h :- 1]
       If h = 0
          RETURN w_
       u_ :+ 1
       If u_ = p
          RETURN ADJOIN([∞, ∞], w_)
```

Wie die folgende Rechnung zeigt, existieren für d=5 tatsächlich rationale Punkte (x,y) mit $y \neq 0$ auf der elliptischen Kurve $y^2 = x^3 - 25x$. Bis zur Höhe h=1000 sind dies:

$$\text{points}(-25, 0, 0, 1000) = \left\{[-5, 0], [-4, \pm 6], \left[-\frac{5}{9}, \pm\frac{100}{27}\right], [0, 0], [5, 0], \left[\frac{25}{4}, \pm\frac{75}{8}\right], [45, \pm 300]\right\}$$

Um auf die zugehörigen Dreiecke zu kommen, verwenden wir die nachfolgende Routine:

$$\texttt{triangle(d, x, y) :=}\ \left[\left|\frac{x^2-d^2}{y}\right|,\ \left|\frac{2\cdot x}{y}\right|\cdot d,\ \frac{x^2+y^2}{|y|}\right]$$

Damit erhält man z.B. für d=5 und die oben berechneten Punkte mit $y \neq 0$ die folgenden zugeordneten Dreiecke:

$$\texttt{TABLE(triangle(5, u}_1\texttt{, u}_2\texttt{), u, SELECT(u}_2 \neq 0\texttt{, u, points(-25, 0, 0, 100)))}$$

$$\begin{bmatrix} [-4, \pm 6] & \left[\frac{3}{2}, \frac{20}{3}, \frac{26}{3}\right] \\ \left[-\frac{5}{9}, \pm\frac{100}{27}\right] & \left[\frac{20}{3}, \frac{3}{2}, \frac{409}{108}\right] \\ \left[\frac{25}{4}, \pm\frac{75}{8}\right] & \left[\frac{3}{2}, \frac{20}{3}, \frac{325}{24}\right] \\ [45, \pm 300] & \left[\frac{20}{3}, \frac{3}{2}, \frac{1227}{4}\right] \end{bmatrix}$$

Wie können wir allgemein für ein quadratfreies d feststellen, ob es kongruent ist oder nicht? Nach dem oben Gesagten, sollte uns bei der Beantwortung dieser Frage der Wert L(E,1) weiterhelfen, welcher sich hier darstellen läßt in der Form (s. [10])

$$L(E,1) = \frac{a(n-2m)^2}{\sqrt{d}}C,$$

wobei die auftretenden Konstanten die Bedeutung bzw. den Wert

$C = 0.163878597\ldots$, $a = 2 - (d \bmod 2)$,

$$n = \#\{(x,y,z) \in \mathbf{Z}^3 \,|\, x^2 + 2ay^2 + 8z^2 = d/a\},\quad m = \#\{(x,y,z) \in \mathbf{Z}^3 \,|\, x^2 + 2ay^2 + 32z^2 = d/a\}$$

haben. Insbesondere ist also $L(E,1) \neq 0$, d.h. d dann noch obigem sicher keine kongruente Zahl, falls $n \neq 2m$ ist. Gilt andererseits n=2m, d.h. L(E,1) = 0, so ist d mit großer (wenn auch nicht mit letzter!) Sicherheit kongruent, da sonst daraus folgen würde, dass die Vermutung von Birch und Swinnerton-Dyer schlicht und einfach falsch ist!

Natürlich lassen wir es uns auch hier wieder nicht nehmen, für die Beantwortung der alles entscheidenden Frage, ob nämlich n=2m für das vorgegebene quadratfreie d gilt oder nicht, eine Derive-Routine zusammen mit einem kleinen Beispiel – die Bestimmung aller quadratfreien d<20, welche kongruent sind – bereitzustellen.

```
solvable?(d, a_, u_, m_ := 0, n_ := 0, x_, y_, u_, v_) :=
  Prog
    a_ := 2 - MOD(d, 2)
    d :/ a_
    u_ := REST(SORT({0, 1, ..., FLOOR(√d)}·{0, 1, ..., FLOOR(√(d/(2·a_)))}))
    Loop
      If u_ = []
        RETURN SOLVE(2·n_ = m_)
      x_ := u_↓1↓1
      y_ := u_↓1↓2
      v_ := x_^2 + 2·a_·y_^2
      z_ := √((d - v_)/8)
      If INTEGER?(z_)
        Prog
          n_ :+ (2 - 0^x_)·(2 - 0^y_)·(2 - 0^z_)
          If EVEN?(z_)
            m_ :+ (2 - 0^x_)·(2 - 0^y_)·(2 - 0^z_)
      u_ := REST(u_)
```

```
TABLE(solvable?(d), d, SELECT(SQUAREFREE(n_), n_, 1, 20))'
```

1	2	3	5	6	7	10	11	13	14	15	17	19
false	false	false	true	true	true	false	false	true	true	true	false	false

Wie daraus unmittelbar folgt, hat für die Zahlen d=1,2,3,10,11,17,19 die elliptische Kurve $y^2 = x^3 - d^2x$ den Rang 0, d.h. E(Q) ist endlich! In den anderen Fällen, wo also der Rang r >0 ist, wäre noch die Frage nach seinem tatsächlichen Wert ausständig, die im allgemeinen jedoch alles andere als einfach zu beantworten ist. Als Faustregel kann man nehmen, dass in diesen Fällen der Rang sehr klein ist, meist sogar nur 1. Tatsächlich ist der Rang für kongruente d<100 nur in 3 Fällen größer als 1, nämlich 2, und zwar für d=34,41 und 65.

In jedem Fall wird dazu eine Routine für die oben eingeführte Punktaddition benötigt, welche nachfolgend gleich für den allgemeinen Fall von zwei Punkten U und V auf einer elliptischen Kurve $y^2 = x^3 + ax + b$ und für K=$\mathbf{F}_p$ bzw. **Q** (d.h. für p=0) bereitgestellt wird. Hierzu muss vorher die eingebaute Routine INVERSE_MOD(n,m) leicht „angepaßt" werden, damit sie auch für m=0 die von uns gewünschten Werte liefert.

```
invmod(n, m) :=
  If m = 0
     1/n
     INVERSE_MOD(n, m)

add(u, v, a, p := 0, k_) :=
  Prog
    If u↓1 + v↓1 = ∞
       If u↓1 = ∞
          RETURN v
          RETURN u
    If u↓1 = v↓1
       Prog
         If MOD(u↓2 + v↓2, p) = 0
            RETURN [∞, ∞]
         k_ := MOD((3·u↓1^2 + a)·invmod(2·u↓2, p), p)
         If k_ = ?
            RETURN GCD(2·u↓2, p)
       Prog
         k_ := MOD((v↓2 - u↓2)·invmod(v↓1 - u↓1, p), p)
         If k_ = ?
            RETURN GCD(v↓1 - u↓1, p)
    v := MOD(k_^2 - u↓1 - v↓1, p)
    [v, MOD(- u↓2 + k_·(u↓1 - v), p)]
```

Um konkret zu zeigen, dass eine elliptische Kurve den Rang 1 hat, muss man die Existenz eines Punktes P von unendlicher Ordnung zeigen, sodass sich jeder Punkt X der elliptischen Kurve darstellen läßt in der Form X= T + nP mit $T \in E(Q)_{tors}$ und n ε **Z**. Als einen solchen Punkt P könnten wir in dem früher betrachteten Beispiel $y^2 = x^3 - 25x$ den Punkt (-4,6) wählen. Tatsächlich gilt dann z.B.

$$\text{add}([0, 0], [-4, 6], -25) = \left[\frac{25}{4}, \frac{75}{8}\right]$$

$$\text{add}([5, 0], [-4, 6], -25) = \left[-\frac{5}{9}, -\frac{100}{27}\right]$$

d.h. diese Punkte lassen sich in der Form T + nP mit T ε {O, (0,0),(-5,0),(5,0)} darstellen. Für n<0 benötigen wir dabei den Punkt –P, der sich durch einfache Vorzeichenänderung der y-Koordinate ergibt. Invertierung bez. + ist also für elliptischen Kurven gewissermaßen „gratis"! Auch dazu noch die kurze Derive-Routine:

```
inv(u, p := 0) :=
  If FIRST(u) = ∞
     u
     [u↓1, MOD(- u↓2, p)]
```

Damit können wir dann definieren

$$nP := \begin{cases} P + \ldots + P \text{ (n - mal)}, \text{falls } n \geq 0 \\ (-P) + \ldots (-P) \text{ (|n| - mal)}, \text{falls } n < 0 \end{cases}$$

Was die Berechnung von nP betrifft, so haben uns bereits die alten Ägypter „vorexerziert", wie man so etwas macht, und zwar am Beispiel der Bildung von additiven Potenzen von natürlichen Zahlen, was dann natürlich auf die Berechnung eines Produkts hinausläuft. Indem man ihr Verfahren z.B. für die Berechnung des Vielfachen 43P von P anwendet, erhält man mit Hilfe der Binärdarstellung von 43

$43P=(2^5+2^3+2^1+2^0)\,P = 2(2(2(2(2P))))+2(2(2P))+2P+P$

Außer der Folge P, 2P, 2(2P), 2(2(2P)),... benötigt man für die praktische Durchführung dieser Rechnung noch die weitere Folge 43,21,10,5,2,1, welche man aus 43 durch fortgesetztes Halbieren und Runden auf die nächstkleinere ganze Zahl erhält. Wird diese Folge nämlich mod 2 betrachtet, was dann also 1,1,0,1,0,1 ergibt, so ist dies in umgekehrter Reihenfolge (!) gerade die Binärdarstellung von $43=(101011)_2$, welche wir für die „richtige" Aufsummierung von Gliedern der Folge P, 2P, 2(2P), 2(2(2P)),... gemäß obiger Formel benötigen.

Und hier nun das Programm zur Berechnung der Vielfachen nU eines Punkts U auf einer elliptischen Kurve $y^2 = x^3 + ax + b$, wobei a und p die gleiche Bedeutung wie schon in add( ) haben. (Insbesondere gibt der Wert von p weiterhin an, ob wir in **Q** oder in $\mathbf{F}_p$ rechnen.)

```
multiple(u, n, a, p := 0, b_) :=
  Prog
    If n < 0
      RETURN multiple(inv(u, p), -n, a, p)
    b_ := [∞, ∞]
    Loop
      If n = 0
        RETURN b_
      If ODD?(n)
        Prog
          b_ := add(u, b_, a, p)
          If NUMBER?(b_)
            RETURN b_
      u := add(u, u, a, p)
      If NUMBER?(u)
        RETURN u
      n := FLOOR(n, 2)
```

```
TABLE(multiple([-4, 6], n, -25), n, 1, 5)
```

$$\begin{bmatrix} 1 & [-4,\ 6] \\ 2 & \left[\frac{1681}{144},\ -\frac{62279}{1728}\right] \\ 3 & \left[-\frac{2439844}{5094049},\ \frac{39601568754}{11497268593}\right] \\ 4 & \left[\frac{11183412793921}{2234116132416},\ \frac{1791076534232245919}{3339324446657665536}\right] \\ 5 & \left[-\frac{506744562502300651 24}{7946713184661354902 5},\ -\frac{2805376007832772561194783839874}{7084044944665570808608396926 25}\right] \end{bmatrix}$$

Die oben gerechneten Vielfachen zeigen auch an, dass die früher definieren „Höhen" der Vielfachen nP mit wachsendem n sehr stark ansteigen. Hier noch zum Abschluß das doch recht beindruckende Dreieck, welches für d=5 dem Vielfachen 5P in obiger Liste entspricht:

$$\text{triangle}\left(5,\ -\frac{506744562502300651 24}{7946713184661354902 5},\ -\frac{2805376007832772561194783839874}{7084044944665570808608396926 25}\right)$$

$$\left[\frac{3940910118004723694 43}{6345828311648907679 0},\ \frac{6345828311648907679 00}{3940910118004723694 43},\ \frac{1134239739242208763759839066962608008653434855037398 2}{2791758439883276098953725936146011887811175624578 75}\right]$$

3. Elliptische Kurven in der Kryptographie

Obwohl es zu dem Themenkomplex „Elliptische Kurven und Diophantische Gleichungen" noch unendlich viel mehr zu sagen gäbe – schließlich wurde bekanntlich ja auch der Beweis von A. Wiles (z.T. gemeinsam mir R,. Taylor) für die berühmt berüchtigte „Fermatsche Vermutung", mit Hilfe von gewissen Elliptischen Kurven geführt –, so möchte ich doch noch kurz auf die Verwendung von Elliptischen Kurven in der Kryptographie eingehen. Damit zusammenhängend spielen Elliptische Kurven, wie wir gleich sehen werden, auch eine wichtige Rolle beim Testen von ganzen Zahlen auf Primalität bzw. bei der Auffindung von nichttrivialen Faktoren von zusammengesetzten Zahlen.

Im Gegensatz zu den bisher betrachteten Beispielen, werden in der Kryptographie elliptische Kurven ausschließlich über endlichen Körpern $\mathbf{F}_q$ mit $q = p^m$ $(p \in \mathbf{P})$ betrachtet, und hier wiederum nur solchen, wo entweder m=1 und p „groß" oder p = 2 ist. Was den ersteren Fall betrifft, haben wir dabei ja schon in der Weise „vorgesorgt", als alle bisher vorgestellten Routinen auch mod p voll funktionieren, was uns nun zugute kommt.

Die Verwendung von Elliptischen Kurven in der Kryptographie basiert auf dem Problem des Diskreten Logarithmus (engl. DLP = Discrete Logarithm Problem). Dieses kann ganz allgemein in beliebigen Gruppen formuliert werden, die Verwendung von Elliptischen Kurven hat aber den entscheidenden Vorteil, dass es bei geschickter Auswahl der Kurven (sog. supersinguläre und anomale Kurven müssen dabei vermieden werden!) es gegenüber dem DLP für andere Gruppen und auch gegenüber dem Faktorisierungsproblem, welches die Basis von RSA bildet (s. [6]), nicht einmal sog. subexponentielle Attacken gibt. Insbesondere kann daher bei vergleichbarer Sicherheit die Schlüssellänge wesentlich kürzer sein. Eine sehr gängige Schlüssellänge ist z.B. 160 Bits, was etwa 1024 Bits bei RSA entspricht! Aufgrund der geringeren Hardwareanforderungen ist ECC (=Elliptic Curve Cryptography) prädestiniert für den Einsatz auf Chipkarten und z.B. gegenüber RSA auch um etwa den Faktor 10 schneller.

Um zu verstehen, worum es beim Problem des Diskreten Logarithmus eigentlich geht, sei nachfolgend eines der ältesten darauf basierenden Chiffrierverfahren vorgestellt, das sog. Schlüsselaustauschverfahren nach Diffie-Hellman aus dem Jahr 1976. Wie der Name schon sagt, stellt es eine Methode dar, wie sich zwei Teilnehmer eines Netzes, nachfolgend Alice and Bob genannt, auf einen gemeinsamen Schlüssel einigen können. Dazu müssen folgende Schritte eingehalten werden.

- Alice und Bob einigen sich auf eine elliptische Kurve E über einen endlichen Körper $\mathbf{F}_q$ (wie oben beschrieben) und auf einen Startpunkt $P \in E$.
- Alice wählt eine geheime ganze Zahl a und sendet aP an Bob.
- Bob wählt seinerseits eine geheime ganze Zahl b und sendet bP an Alice.
- Alice berechnet den Schlüssel $x = a(bP)$.
- Bob berechnet den Schlüssel $x = b(aP)$.
- Der gemeinsame Schlüssel x enthält dann in codierter Form alle Informationen, mit deren Hilfe in der Folge nach einem gängigen traditionellen Verfahren Nachrichten zwischen Alice und Bob verschlüsselt werden können.

Die Sicherheit des Verfahrens basiert auf der Schwierigkeit des ECDLP (=Elliptic Curve Discrete Logarithm Problem): Bei geeigneter Wahl der Parameter – wie schon erwähnt sollte insbesondere q nach heutigen Maßstäben mindestens 160 Bits haben - ist es sehr schwer bzw. praktisch unmöglich, aus P and aP bzw. bP die Zahlen a und b zu berechnen! Andere wichtige Chiffrierverfahren, die auf DLP basieren und für die es dementsprechend auch eine „ECDLP-

Variante“ gibt sind das ElGamal-Verfahren und das Verfahren von Massey-Omura (siehe dazu [6]).

Bekannte Attacken auf das ECDLP sind die nachfolgenden (wobei die beiden erstgenannten auch auf das allgemeine DLP in Gruppen anwendbar sind und zwar mit einem Aufwand, der stets proportional zu $\sqrt{p}$ mit p als dem größten Primteiler von #E ist):

- Pollard's ≡-Methode
- Shanks' „Baby-step Giant-step“- Methode
- MOV-Attacke (nach Menezes, Okamoto, Vanstone) , welche für supersinguläre Kurven, d.h. Kurven mit $\#E(\mathbf{F}_q) \equiv q+1 \bmod p$, ECDLP in Subexponentialzeit lösen kann
- Anomale Kurven Attacke (Kurven mit $\#E(\mathbf{F}_q) = q$), für welche ECDLP mit Hilfe von sog. p-adischen Zahlen gelöst werden kann

Was die Auswahl der Parameter für die elliptische Kurve betrifft, gibt es da vor allem eine Schwierigkeit. Man muss unbedingt sicherstellen, dass der Basispunkt P eine hohe Ordnung besitzt, was darauf hinausläuft, dass die Anzahl #E der Punkte für die zugrundegelegte elliptische Kurve E durch eine große Primzahl teilbar sein sollte, welche höchstens um einige Stellen kleiner als #E ist. Trifft dies nämlich nicht zu, so gibt es dann auch noch die Attacke von Pohlig-Hellman auf ECDLP, welche zwar im Normalfall völlig harmlos ist, aber genau diese Schwachstelle höchst effizient ausnützt,.

Um ganz sicher zu gehen, dass # $E(\mathbf{F}_q)$ nicht „glatt“ ist, d.h. nicht nur relativ kleine Primfaktoren besitzt, sollte man also $\#E(\mathbf{F}_q)$ auf jeden Fall berechnen. Dies ist möglich, wenn auch nicht ganz einfach. Wir werden nachfolgend wieder für den Spezialfall m=1, d.h. dass q = p eine Primzahl ist, zwei grundverschieden Ansätze dazu skizzieren.

Der erste besteht darin, dass man eine ausreichend große (z.B. 50-stellige) Primzahl p und eine elliptische Kurve E: $y^2 = x^3 + ax + b \bmod p$ vorgibt und dazu $\#E(\mathbf{F}_p)$ bestimmt. Eine naive Möglichkeit dazu, welche allerdings für Primzahlen dieser Größenordung sicher nicht in Frage kommt, bestünde nun darin, alle in Frage kommenden x-Werte, nämlich x=0,1,2,..,p-1 daraufhin zu überprüfen, ob es keinen, einen oder zwei y-Werte dazu gibt und diese Lösungszahlen (vermehrt um 1 für den Punkt O) aufzuaddieren. Für kleine Beispiele, etwa $p<10^6$, wäre diese Methode aber noch durchaus ausreichend, weshalb nachfolgend das kurze Programm dazu angegeben ist.

```
card(a, b, p) := p + 1 + Σ(MODS((x^3 + a·x + b)^((p - 1)/2), p), x, 0, p - 1, 1)

card(1, 2, 10^5 + 3) = 100152

card(1, 2, 10^6 + 3) = 999328
```

(Die Rechenzeiten für die beiden Beispiele betrugen dabei übrigens 12.6s bzw. 193.6s auf meinen 2GHz-PC.)

Eine schon etwas bessere Methode, wenngleich in unserem Fall ebenfalls noch nicht ausreichend, besteht darin, das sog. „Hasseintervall“

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

in dem ja nach dem schon zitierten Satz von Hasse $\#E(\mathbf{F}_p)$ jedenfalls liegen muss, systematisch auf alle Zahlen n hin zu durchsuchen, sodass für einen vorher ausgewählten Punkt P gilt nP=O. Aus diesem n kann dann leicht auch die Ordnung von P gewinnen, indem man für jeden Primteiler r von n, für welchen ebenfalls (n/r)P=O gilt, n durch n/r ersetzt,

solange dies möglich ist. Das resultierende n muss dann ord(P) sein. Ist dann ord(P)> $4\sqrt{p}$, was in der Praxis fast immer zutrifft, so ist das zu Beginn gefundene n das einzige Vielfache von ord(P) im Hasseintervall und daher die gesuchte Anzahl $\#E(\mathbf{F}_p)$. Ist obige Bedingung für ord(P) nicht erfüllt, so könnte dann z.B. das Ganze für einen anderen Punkt P wiederholen oder nach mehreren Fehlversuchen auch zum sog. „quadratischen Twist" $\overline{E}$ von E übergehen, der die Gleichung

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

besitzt, wobei g ein fix gewählter quadratischer Nichtrest mod p ist, d.h. die Kongruenz $x^2 \equiv g \bmod p$ darf für dieses g nicht lösbar sein! Wie nämlich Mestre gezeigt hat, funktioniert dann obiges Verfahren zur Bestimmung der Punkteanzahl für p > 229 entweder für E selbst oder für $\overline{E}$ sicher, womit man dann gemäß der leicht zu beweisenden Formel

$$\#E(\mathbf{F}_p) + \#\overline{E}(\mathbf{F}_p) = 2(p+1)$$

auch die Ordnung der jeweils anderen Kurve kennt!

Die folgende Routine dient sowohl zur Bestimmung der Ordnung eines Punkts U auf der elliptischen Kurve, welche wieder durch U und a festgelegt ist, wenn nämlich s den Defaultwert 1 hat, als auch zur Bestimmung von $\#E(\mathbf{F}_p)$ (mit der „Schalterstellung" s=2, jedoch nur dann, wenn U gemäß dem oben Gesagten geeignet, d.h. ord(U) „nicht zu klein ist"). Mit s=0 erhält man dagegen nur irgendein n im Hasseintervall mit nU=O, was für viele Zwecke nützlich und ausreichend ist. Der verwendete Algorithmus ist dabei im wesentlichen die „Baby-step Giant-step"- Methode von Shanks, die auch schon oben im Zusammenhang mit DLP erwähnt wurde. (Einzelheiten dazu entnehme man am besten dem Programm selbst.)

```
ord(u, a, p, s := 1, i_ := 0, j_ := 1, n_, u_, v_, w_, x_, y_) :=
  Prog
    n_ := CEILING(p^(1/4))
    v_ := ITERATES(add(u, t_, a, p), t_, multiple(u, p + 1, a, p), n_ - 1)
    x_ := v_ COL 1
    y_ := v_ COL 2
    w_ := multiple(u, n_, a, p)
    u_ := [∞, ∞]
    Loop
      If MEMBER?(FIRST(u_), x_)
         Loop
           If FIRST(u_) = FIRST(x_)
              Prog
                u_ := IF(u_↓2 = y_↓1, p - i_·n_ + j_, p + i_·n_ + j_)
                If s = 0
                   RETURN u_
                v_ := (FACTORS(u_)) COL 1
                w_ := u_
                Loop
                  x_ := Π(SELECT(multiple(u, u_/t_, a, p) = [∞, ∞], t_, v_))
                  If x_ = 1
                     RETURN IF(s = 1, u_, IF(u_ > 4·√p, w_))
                  u_ :/ x_
                  v_ := SELECT(MOD(u_, t_) = 0, t_, v_)
           x_ := REST(x_)
           y_ := REST(y_)
           j_ :+ 1
      u_ := add(u_, w_, a, p)
      i_ :+ 1
```

Damit lassen sich nun auch schon etwas größere Beispiele rechnen, in denen p bis zu etwa 18-20 Stellen haben darf, je nach vorhandenem Speicher. Wir werden diese Routine weiter unten gleich benötigen, rechnen aber vorher noch das Beispiel von vorhin mit $p=10^5+3$ und U=[1,2].

```
                    6
ord([1, 2], 1, 10  + 3, 0) = 1000004
```

```
ord([1, 2], 1, 10^6 + 3, 1) = 4

ord([1, 2], 1, 10^6 + 3, 2) = ?
```

Wie man sehen kann, hat der Punkt die tatsächliche Ordnung 4, ist also für unsere Zwecke gänzlich ungeeignet. Aber mit der Routine points( ) lassen wir uns einige weitere Punkte anzeigen und werden bald wie folgt „fündig". (Die eigentliche Berechnung von #E dauerte dabei jetzt nur mehr 0.09s !)

```
points(1, 2, 10^6 + 3, 3) = {[1, 2], [1, 1000001], [5, 342322]}

ord([5, 342322], 1, 10^6 + 3, 1) = 499664

ord([5, 342322], 1, 10^6 + 3, 2) = 999328
```

Leider sind wir aber von unserem Ziel #E für ca. 50-stellige Primzahlen berechnen zu können, noch weit entfernt. Dies gelingt erst mit fortgeschritteneren Methoden, wie dem recht aufwändigen Algorithmus von Schoof (s.[9]), der mit einer Komplexität von $O((\ln p)^8)$ immerhin zur Klasse der sog. Polynomialzeitalgorithmen gehört. Elkies und Atkins konnten den Algorithmus von Schoof in der Folge noch weiter auf $O((\ln p)^6)$ verbessern und das Ergebnis wird heute in der Literatur nach ihnen SEA-Algorithmus genannt (siehe [2]). Damit gelingt die Berechnug von #E für mehrhunderstelliges p (und sogar noch weit darüber hinaus) völlig problemlos. Leider verbietet sich die Darstellung des Algorithmus in diesem Rahmen.

Ich möchte statt dessen doch noch kurz auf den oben angekündigten zweiten Ansatz zur Lösung des Problems eingehen, der darin besteht, dass man sich der Auswahl der elliptischen Kurven von vornherein auf einen gewissen Kurventyp, nämlich sog CM-Kurven beschränkt (CM steht dabei für „complex multiplication" ohne dass ich hier auf die Bedeutung dieser Namensgebung näher eingehen kann), für die man relativ einfache Formeln kennt, mit deren Hilfe man ihre Punkteanzahl dann leicht bestimmen kann. Ein einfaches Beispiel in dieser Richtung, ist der folgende bereits von Gauß bewiesene

Satz: Ist die elliptische Kurve E von der Bauart $y^2 = x^3 + ax$ über $\mathbf{F}_p$, so hat man zwei Fälle zu unterscheiden:

1. Supersingulärer Fall: Ist $p \equiv 3 \bmod 4$, so gilt $\#E(\mathbf{F}_p) = p + 1$.

2. CM-Fall: Ist $p \equiv 1 \bmod 4$ und $p = u^2 + v^2$, so gilt $\#E(\mathbf{F}_p) \in \{p+1 \pm 2u, p+1 \pm 2v\}$.

Allgemeiner geht man zur der Konstruktion von CM-Kurven mit bereits vorher feststehender Ordnung so vor, dass man aus einer Zahlenreihe von Zahlen D mit $D < 0$ und $D \equiv 0,1 \bmod 4$, nämlich

-3, -4, -7, -8, -11, -19, -43, -67, -163, -15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -123, -148, -187, -232, -235, -267, -403, -427,...

(für den Eingeweihten sind dies übrigens die negativen Diskriminanten D mit $D \equiv 0,1 \bmod 4$ von binären quadratischen Formen nach aufsteigender Klassenzahl h(D) und Absolutgröße geordnet) in der vorgegebenen Reihenfolge nach diejenigen auswählt, für welche die Diophantische Gleichung

$$x^2 + |D|y^2 = 4p$$

lösbar ist. Ein offensichtliche notwendige Bedingung für die Lösbarkeit ist dabei, dass D ein quadratischer Rest mod p ist. Ist diese Vorbedingung erfüllt, so ist die Wahrscheinlichkeit für die Lösbarkeit gegeben durch 1/h(D), was mit ein Grund für obige Anordnung der D-Werte ist. Glücklicherweise ist die Auffindung der Lösungen, falls solche existieren, in der Praxis

überhaupt kein Problem, da man für diesen Zweck den höchst leistungsfähigen Algorithmus von Cornacchia-Smith zur Verfügung hat. Wer nachfolgendes Programm dazu analysiert, wird übrigens überraschenderweise Elemente des Euklidischen Algorithmus darin entdecken.

```
CS(p, D, a_, b_, c_, r_) :=
  Prog
    If JACOBI(D, p) < 1
      RETURN false
    b_ := SQUARE_ROOT(D, p)
    If ODD?(b_ - D)
      b_ := p - b_
    a_ := 2·p
    c_ := FLOOR(2·√p)
    Loop
      If b_ ≤ c_ exit
      r_ := MOD(a_, b_)
      a_ := b_
      b_ := r_
    a_ := 4·p - b_^2
    If MOD(a_, ABS(D)) > 0
      RETURN false
    c_ := √(a_/ABS(D))
    If ¬ INTEGER?(c_)
      RETURN false
    [±b_, ±c_]
```

Hat man zu einem D obiger Liste mit Hilfe dieses Programms ganzzahlige Lösungen $x=\pm u$, $y=\pm v$ von obiger Diophantischer Gleichung gefunden, so kann man ähnlich wie im CM-Fall des Satzes von Gauß eine Liste von „Kandidaten" der Kurvenordnung und dazugehörige Kurven sofort angeben (für Einzelheiten siehe [2]).

Übrigens findet sich hier der CM-Fall des Satzes von Gauß für D = –4 wieder, d.h. man hat hier die Diophantische Gleichung $x^2+4y^2=4p$ zu lösen und die Kurvenordnung ergibt sich dann als eine der vier Zahlen $p+1\pm u$, $p+1\pm 2v$, wobei $u^2+4v^2=4p$. Nachfolgend ein einfaches Beispiel dazu, wofür wir die CM-Kurve $y^2=x^3+3x$ und eine zufällig ausgewählte 50-stellige Primzahl p der Form 4k+1 gewählt haben.

```
(p := NEXT_PRIME(RANDOM(10^50))) = 33977458290450187620247948554055471607720687203261

[DIM(p), MOD(p, 4)] = [50, 1]

CS(p, -4) = [±1097625800944881641040321Ø, ±19641533336154955701056Ø6]

[u := 1097625800944881641040321Ø, v := 19641533336154955701056Ø6]

points(3, Ø, p, 3) = {[Ø, Ø], [1, 2], [1, 33977458290450187620247948554055471607720687203259]}

P := [1, 2]
SELECT(multiple(P, n, 3, p) = [∞, ∞], n, [p + 1 + u, p + 1 - u, p + 1 + 2·v, p + 1 - 2·v]) =
  [33977458290450187620247937577797462158904276800052]

N := 33977458290450187620247937577797462158904276800052

FACTOR(N) = 2^2·13·8644633·75585934004570740864587350097403392368297

r := 75585934004570740864587350097403392368297

[DIM(r), DIM(N)] = [41, 50]
```

Wie man aus obigen Rechnungen ersehen kann, ist auch die Kurvenordnung, welche oben mit N bezeichnet wurde, 50-stellig und enthält einen 41-stelligen Primfaktor r, was für Zwecke der Kryptographie mehr als ausreichen sollte.

Um diese Daten zu erhalten, musste hier eine 50-stellige Zahl faktorisiert werden, was i.allg. schon nicht mehr ganz einfach ist. Dies gibt mir Gelegenheit darauf hinzuweisen, dass Derive

intern zum Faktorisieren mehrere Methoden abwechselnd verwendet, wobei eine davon auch ECM (= Elliptic Curve Method) ist, eine von H.W.Lenstra jr. (s. [5]) im Jahre 1985 eingeführte Faktorisierungsmethode, welche ebenfalls auf elliptischen Kurven basiert.

Um ECM besser zu verstehen, machen wir folgendes Gedankenexperiment. Was würde eigentlich passieren, wenn wir in add(u,v,a,p) bzw. multiple(u,n,a,p) für den Parameter p, von dem wir bisher immer angenommen hatten, dass er 0 oder prim ist, eine zusammengesetzte Zahl n einsetzen? Wenn man sich dazu die definierenden Gleichungen für die Punktaddition noch einmal genauer ansieht, wird man feststellen, dass dann die Variable k nicht mehr notwendigerweise definiert sein wird, nämlich dann nicht, wenn die auftretenden Nenner $x_2 - x_1$ bzw. $2y_1$ mod p nicht invertierbar sind, d.h. wenn gilt $ggT(x_2 - x_1, p) > 1$ bzw. $ggT(2y_1, p) > 1$. Unsere Routinen sind dabei schon vorsorglich so geschrieben worden, dass sie in diesem Fall diese ggT ausgeben, welche i.allg. nichttriviale Teiler von n darstellen.

Der Grundgedanke von ECM ist nun kurz gesagt der, genau diesen Fall zu provozieren, indem man für eine vorgegebene elliptische Kurve E und einen Punkt $P \in E$ ein geeignetes Vielfaches mP „mod N" berechnet und hofft, dass dies in der beschriebenen Weise zu einem Teiler von n führt. Die Chancen dafür sind dann recht gut, wenn es einen Primteiler q von N gibt, sodass $\#E(\mathbf{F}_q)$ "glatt", d.h. keine wirklich großen Primteiler besitzt, da dann ein m der Form m=kgV(1,2,..,B) für eine nicht zu große Schranke B den Zweck erfüllen wird.

Zurückkehrend zu unserem Beispiel wollen wir annehmen, wir hätten die kleinen Teiler 4 und 13 durch Probedivision schon gefunden. Der zweitgrößte Primteiler ergibt sich dann wie folgt:

$$\text{multiple}\left([1,\ 1],\ \text{LCM}([1,\ ...,\ 1000]),\ 17,\ \frac{N}{4 \cdot 13}\right) = 8644633$$

Wie die nachfolgende Rechnung zeigt, führte dies hier deshalb zum Erfolg, weil für die gewählten Parameter die Ordnung vom Punkt (1,1) in $E(\mathbf{F}_{8644633})$ bemerkenswert glatt ist:

$$\text{FACTOR}(\text{ord}([1,\ 1],\ 17,\ 8644633)) = 7^3 \cdot 11 \cdot 29 \cdot 79$$

Hier noch ein etwas größeres Beispiel, nämlich die Faktorisierung der Fermatzahl F_8, was insbesondere auch die Leistungsfähigkeit der Routine ord( ) nochmals schön aufzeigt:

$$\text{multiple}\left([1,\ 1],\ \text{LCM}([1,\ ...,\ 7000]),\ 134,\ 2^{2^8} + 1\right) = 1238926361552897$$

$$\text{FACTOR}(\text{ord}([1,\ 1],\ 134,\ 1238926361552897)) = 3 \cdot 5 \cdot 19 \cdot 47 \cdot 2557 \cdot 5237 \cdot 6907$$

Auch wenn es dann im Detail noch sehr viele Feinheiten der Implementierung gibt (s. z.B. [7]), insbesondere auch was die Berechnung von mP betrifft, die in der Praxis gewissermaßen „scheibchenweise" erfolgt, so gibt es zur Grundidee von ECM nicht viel mehr zu sagen! Sie gehört übrigens zur Klasse der subexponentiellen Faktorisierungsmethoden und es können damit Primfaktoren bis etwa 40 Stellen gefunden werden, in Einzelfällen auch noch weit darüber hinaus!

Eine letzte Frage bezüglich unseres 41-stelligen Primfaktors r von N bleibt noch zu klären: Können wir uns auch wirklich ganz sicher sein, dass r prim ist? Schließlich erfolgt die Feststellung der Primalität in Derive (wie auch in jedem anderen CAS!) standardmäßig mit Hilfe probabilistischer Primzahltests, wobei also rein theoretisch (mit einer allerdings sehr kleinen Wahrscheinlichkeit!) zusammengesetzte Zahlen als prim ausgewiesen werden können. Will man diesen letzten Rest an Unsicherheit beseitigen, so muss man noch zusätzlich einen streng deterministischen Primzahltest anwenden. Dafür gibt es mehrere

Möglichkeiten, eine davon – der Leser hat es längst erraten! – basiert wiederum auf elliptische Kurven. Theoretische Grundlage dafür ist der folgende (s. [3])

Satz (Goldwasser-Kilian): Sei N > 1 eine natürliche Zahl mit ggT(6,N)=1 und sei E die Menge der Punkte (x,y), welche eine Gleichung

$$y^2 = x^3 + ax + b \bmod N$$

mit gewissen ganzen Zahlen a,b erfüllen, wobei $ggT(4a^3 + 27b^2, N) = 1$ sei. Gibt es dann ein $m \in \mathbf{N}$ und einen Primteiler $q > (\sqrt[4]{N} + 1)^2$ von m, sowie einen Punkt P von E, sodass mit der wie für eine elliptische Kurve erklärten Addition gilt

$$mP = O, \text{ aber } (m/q)P \neq O$$

so ist N prim.

Prinzipiell ist dazu noch zu sagen, dass dieser Test natürlich erst zur Anwendung kommt, wenn N schon eine Reihe von einfachen probalistischen Primzahltests bestanden hat, sodass also mit hoher Wahrscheinlichkeit N wirklich prim ist und man auf einer „echten" elliptischen Kurve rechnet. Eventuell daraus resultierende Probleme würden gerade die Zusammengesetztheit von N beweisen! Dies gilt insbesondere auch für die Berechnung von m, für welches man üblicherweise m = #E nimmt, wobei E am einfachsten wieder als CM-Kurve angenommen wird.

Eine weitere Hürde ist ferner die Auffindung eines „genügend großen" Primteilers q von m, falls ein solcher existiert. Dabei wird man in der Regel sich zunächst damit begnügen, dass q eine wahrscheinliche Primzahl ist, und erst nach bestandenen Test sich der Frage der Primalität von q erneut zuwenden, indem man zeigt, dass auch q den Goldwasser-Kilian-Test besteht. Da die q's exponentiell abnehmen, werden sie schnell so klein, dass der Nachweis der Primalität dann kein Problem mehr ist.

Die Gesamtheit aller Parameter, welche für die Tests verwendet wurden, bildet dann übrigens ein sog. Primzahlzertifikat, das eine eventuelle Wiederholung oder Überprüfung des Tests sehr einfach macht. Dies ist der Hauptvorteil gegenüber den sog. APRCL-Test, einem ebenfalls sehr leistungsfähigen deterministischen Primzahltest (s. [1]).

Es sei auch noch erwähnt, dass der derzeitige „Rekord" (Juli 2003) für eine deterministisch getestete Primzahl allgemeiner Bauart (nämlich die Primzahl $(32*10^{6959} - 23)/99$ mit immerhin 6959 Stellen!) von dieser Methode gehalten wird, zu der außer Goldwasser-Kilian auch noch Atkin und Morain wichtige Beiträge geleistet haben, und die heute unter der allgemeinen Bezeichnung ECPP (=Elliptic Curve Primality Proving) zusammengefaßt wird.

Abschließend noch ein etwas kleineres Beispiel, nämlich die Anwendung obiger Überlegung auf unser 41-stelliges r von unserem obigen Beispiel. Wegen $r \equiv 1 \bmod 4$ kann man ähnlich wie oben (und unter Verwendung der gleichen Kurve und des gleichen Punkts) $\#E(\mathbf{F}_r)$ berechnen und daraus die im Satz verlangten Werte von m und q bestimmen.

```
CS(r, -4) = [±492242655651773727152, ±122516227471274471789]

[u := 492242655651773727152, v := 122516227471274471789]

SELECT(multiple([1, 2], N, 3, r) = [∞, ∞], N, [r + 1 + u, r + 1 - u, r + 1 + 2·v, r + 1 - 2·v]) =
  [7558593400457074086409510744175161864114 6]

m := 7558593400457074086409510744175161864114 6

FACTOR(m) = 2·13·146009·199107678832681918090652755972765 69

q := 199107678832681918090652755972765 69
```

$$\text{SOLVE}(q > (r^{1/4} + 1)^2) = \text{true}$$

$$\text{multiple}([1, 2], m, 3, r) = [\infty, \infty]$$

$$\text{multiple}\left([1, 2], \frac{n}{q}, 3, r\right) = [1414598261955364783294645666832814774995 9, 5649346330843816703996721709178518327729 3]$$

Wie aus obigen Rechnungen folgt, sind also die Voraussetzungen des Satzes mit diesen Parametern tatsächlich erfüllt, woraus folgt, dass unser 41-stelliges r somit genau dann prim ist, wenn dies für obiges 35-stelliges q gilt. In dieser Weise macht man dann mit q anstelle von r weiter, was ich hier aber nicht mehr weiter ausführen will.

Obwohl hier viele wichtige Fakten über elliptische Kurven überhaupt nicht zur Sprache gekommen sind, - nochmals sei an das Eingangszitat aus berufenerem Munde erinnert, - hoffe ich doch damit einen kleinen Einblick gegeben zu haben in die wahrlich faszinierende Welt dieser Kurven und ihren vielfältigen Anwendungsmöglichkeiten. Insbesondere ist es meine ganz große Hoffnung, dass die mit viel Liebe zusammengestellten und in ihrem Bereich doch erstaunlich leistungsfähigen Derive-Programme (welche ich übrigens auf Anforderung auch gerne zuschicke!) den interessierten Leser dazu anregen mögen, vieles von dem, was hier nur angedeutet wurde, auf eigene Faust zu erkunden. Für Anregungen und Verbesserungsvorschläge bin ich jederzeit dankbar!

Literatur

[1] L.Adleman, C.Pomerance, and R.Rumely, "On distinguishing prime numbers from composite numbers", Ann. of Math., 117(1983), 173-206.

[2] R.Crandall and C.Pomerance, *Prime numbers: a computational perspective*, Springer-Verlag, 2001

[3] S.Goldwasser and J.Kilian, "Almost all primes can be quickly certified", Proc. 18th Annual ACM Symposium on Theory of Computing, 1986, 316-329.

[4] S.Lang, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, 1978.

[5] H.W.Lenstra, Jr., „Factoring integers with elliptic curves", Annals of Math. (2) 126 (1987), 649-673.

[6] A.Menezes, P.van Oorschot, and S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997 (s. auch http://www.cacr.math.uwaterloo.ca/hac/)

[7] P. Montgomery, "Speeding the Pollard and elliptic curve methods of factorization", Math. Comp. 48(1987), 243-264.

[8] J.H.Silverman and J.Tate, *Rational points on elliptic curves*, Springer-Verlag, 1992

[9] R.Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", Math. Comp. 44(1985), 483-494.

[10] J.B.Tunnell, „A classical Diophantine problem and modular forms of weight 3/2", Inventiones Mathematicae, 72(1983), 323-334.

Anschrift des Verfassers

Ao. Prof. DI Dr. Johann Wiesenbauer
(j.wiesenbauer@tuwien.ac.at)

Institut für Algebra und Computermathematik
der Technischen Universität Wien
Wiedner Hauptstr. 8-10
A-1040 Wien