"... und wozu das alles?" ist eine (von vielen) Frage(n), die sich sicher schon fast jeder Schüler der 7B oder 7C(Rg) einmal gestellt hat, als es nach der Schularbeit Ende März (7C) bzw. Anfang April (7B) mit dem Differenzieren dennoch kein Ende genommen hat, und noch dazu "Kubische Kurven". Bei den anschließenden Optimierungsaufgaben liegen die Anwendungen – wie ihr zweifelsohne zugeben müsst! – auf der Hand, bei den kubischen Kurven eher weniger[1], deshalb nebst meiner im Unterricht eingestreuten Bemerkungen (nicht nur!) für Interessierte folgenden einer mathematischen Zeitschrift (Ja, auch so etwas gibt es. ☺ Mehr noch gibt es deren gar viele ...) entnommen Artikel:

Lenstras Elliptische Kurven-Methode

von Theo de Jong

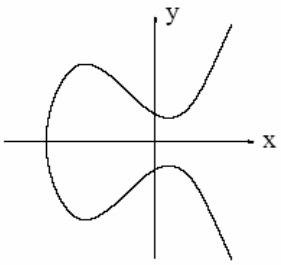
In der Schule lernt ihr, wie man große Zahlen faktorisieren kann. Haben wir z.B. die Zahl $n = 341$, dann probieren wir einfach die Primfaktoren durch und stellen schnell fest, dass 341 zwar nicht durch $2, 3, 5, 7$ teilbar ist, wohl aber durch 11. Damit haben wir $341 = 11 \cdot 31$ gefunden.
Wenn wir Faktoren von n finden wollen, brauchen wir nur die Primfaktoren bis $\sqrt{n}$ zu betrachten. Diese Methode nennt man Probedivision, und sie ist nur für nicht allzu große Zahlen durchführbar.
Nehmen wir z.B. an, dass n eine Zahl mit 19 Dezimalstellen ist. Um die Probedivision durchzuführen, brauchen wir alle Primzahlen bis ungefähr 10^{10}, und davon gibt es genau $455\,052\,511$.
Es stellt sich das Problem, wie man diese speichern sollte. Selbst mit Computern ist es nicht vernünftig, Zahlen n von mehr als 10 Dezimalstellen mit Probedivision zu faktorisieren.
Es gibt verschiedene moderne Faktorisierungsmethoden, die für große Zahlen viel besser funktionieren als die Probedivision. Hier wollen wir eine besprechen, nämlich **Lenstras Elliptische Kurven-Methode**, die 1985 von Lenstra vorgeschlagen wurde.

1. Elliptische Kurven

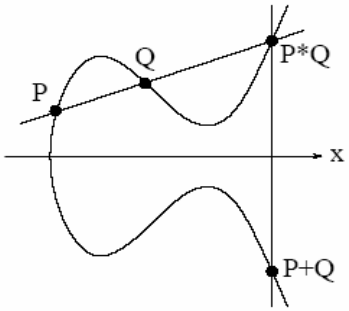
Wir erklären zunächst, was eine elliptische Kurve ist. Nehmen wir reelle Zahlen a, b und betrachten die folgende Menge:

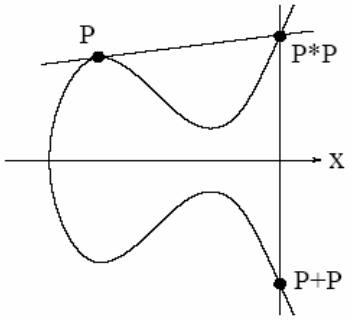
$$E_{a,b} = \{(x, y) | y^2 = x^3 + ax + b\},$$

also die Menge aller Paare (x, y), die die Gleichung $y^2 = x^3 + ax + b$ lösen.
So eine Kurve $E_{a,b}$ könnte wie im nebenstehenden Bild aussehen.



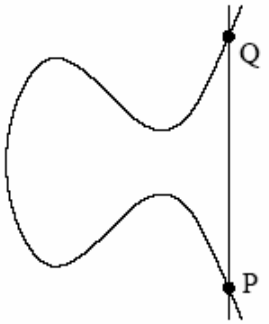
Wir können, wenn Punkte P, Q auf $E_{a,b}$ gegeben sind, einen neuen Punkt, die *Summe* $P + Q$ auf $E_{a,b}$ finden: Man nimmt die Gerade durch P und Q, findet den dritten Schnittpunkt $P * Q$ mit der Kurve, und spiegelt an der $x - Achse$.
Selbst für $P = Q$ kann man etwas machen: Um $P + P = 2P$ zu definieren, nimmt man die Tangente in P an die elliptische Kurve, findet erneut den dritten Schnittpunkt und spiegelt.





[1]: Ein kluger Mensch hat einmal gesagt, dass die theoretische Mathematik von heute die angewandte Mathematik von morgen ist. Dem ist wohl nichts hinzuzufügen, außer vielleicht …, ☺
… dass sogar der n-dimensionale Würfel (der ja – völlig zu Unrecht! – verdächtig nach Hirngespinsten im mathematischen Elfenbeinturm klingt) bei Kommunikationsprozessen (aber nicht im psychologischen Sinn!) eine Anwendung findet!

Es lässt sich zeigen, dass die Addition das Kommutativitätsgesetz $P+Q = Q+P$ und auch das Assoziativitätsgesetz $(P+Q)+R = P+(Q+R)$ erfüllt. Bemerke, dass diese Konstruktion **schief** geht für den Fall, dass P und Q gespiegelt voneinander bezüglich der x–Achse liegen. Dann hat die Gerade durch P und Q nämlich nur *zwei* Punkte mit der elliptischen Kurve gemein. Diese Tatsache hat Lenstra bei seiner Faktorisierungsmethode ausgenutzt.



Formeln für die Addition sind leicht hinzuschreiben. Sind $P=(x_1,y_1)$ und $Q=(x_2,y_2)$ Punkte auf $E_{a,b}$ dann gilt, wie man berechnen kann, $P+Q=(x_3,y_3)$ mit

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned}$$

wobei m die Steigung der Geraden durch P und Q ist bzw. die Steigung der Tangente an die elliptische Kurve in P. Man hat dabei

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \qquad \text{falls } P \neq Q,$$

$$m = \frac{3x_1^2 + a}{2y_1}, \qquad \text{falls } P = Q.$$

Man sieht, dass $P+Q$ genau dann nicht definiert ist, wenn die Steigung der Gerade durch P und Q unendlich ist, also die Gerade durch P und Q vertikal ist.

2. Rechnen Modulo n

Sind a und n gegebene natürliche Zahlen, so schreiben wir $a \bmod n$ für den Rest bei Teilung von a durch n. Also z.B.

$$11 \bmod 2 = 1; \quad 15 \bmod 4 = 3; \quad 98 \bmod 14 = 0.$$

Dann können wir auch modulo n addieren, zum Beispiel

$$23 + 41 \bmod 13 = 12; \quad 1 + 1 \bmod 2 = 0; \quad 45 + 12 \bmod 11 = 2.$$

Multiplizieren modulo n geht auch:

$$4 \cdot 7 \bmod 25 = 3; \quad 8 \cdot 9 \bmod 71 = 1.$$

Kann man auch dividieren? Nun ja, manchmal:

$1/5 \bmod 7 = 3$, da $3 \cdot 5 \bmod 7 = 1$; $\quad 1/2 \bmod 341 = 171$, da $2 \cdot 171 \bmod 341 = 1$.

Aber es gelingt nicht, $1/22 \bmod 341$ zu berechen. Gäbe es nämlich einen Wert x mit $x \cdot 22 \bmod 341 = 1$, dann multiplizieren wir beide Seiten mit 31. Nun ist $22 \cdot 31 = 682 = 0$ (alles $\bmod 341$), also würde folgen

$$0 = x \cdot 22 \cdot 31 = 1 \cdot 31 = 31 \ (\text{ alles } \bmod 341),$$

also $0 \bmod 341 = 31$ was natürlich Unsinn ist. Also kann es so ein x nicht geben. Der wirkliche Grund dürfte klar sein: die Zahl 22 hat mit 341 einen gemeinsamen Teiler. Es gilt nämlich:

Satz: $\qquad 1/a \bmod n$ existiert **nicht** $\iff \mathrm{ggT}(a,n) > 1.$

Es gibt schnelle Verfahren, um den Kehrwert von a modulo n, wenn dieser existiert, auszurechnen.

3. Lenstras Methode

Wie können wir nun elliptische Kurven benutzen, um damit eine Zahl n zu faktoriseren? Lenstras Idee ist es, eine elliptische Kurve $E_{a,b}$ mit $a, b \in \mathbb{N}$ und einen Punkt P darauf zu wählen. Man könnte z.B eine Zufallszahl a wählen, $P = (2, 1)$ und $b = -2a - 7$. Nun nimmt man einen große Zahl s und versucht

$$(x_s, y_s) = sP = \underbrace{P + \cdots + P}_{s\text{-fach}}$$

zu berechen, nun aber nicht mit reellen Zahlen, sondern modulo n, der zu faktorisierenden Zahl. Man hofft dabei, dass die Berechnung irgendwann zusammenbricht. Der Grund dafür wäre, dass bei der Berechnung einer "Steigung einer Geraden" die Division modulo n nicht aufgeht. Wie im letzten Abschnitt erklärt, ist der Grund dafür, dass dann der Nenner und n einen gemeinsamen Teiler haben, den wir mit dem euklidischen Algorithmus schnell berechnen können.

Beispiel: Natürlich sollte man den Rechner diese Berechnungen durchführen lassen. Weil wir die Methode illustrieren wollen, nehmen wir aber ein kleines n, nämlich $n = 1003$, $P = (2, 1)$ und die elliptische Kurve $y^2 = x^3 + x - 9$. Wir berechnen $72P \bmod 1003$.

$2P$	$= (289, 641)$	$16P$	$= (64, 719)$
$4P$	$= (314, 713)$	$32P$	$= (550, 949)$
$8P$	$= (571, 704)$	$64P$	$= (276, 114)$

Nun müssen wir $8P + 64P$ berechnen. Dafür brauchen wir den Kehrwert von $x_{64} - x_8 = 276 - 571 = -295 = 708$ (alles $\bmod 1003$. Den gibt es aber nicht, da 1003 und 708 einen gemeinsamen Teiler haben. Diesen können wir mit dem euklidischen Algorithmus, der besagt, dass für alle a, b gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a - b)$, berechnen:

$$\mathrm{ggT}(1003, 708) = \mathrm{ggT}(708, 295) = \mathrm{ggT}(413, 295) = \mathrm{ggT}(108, 295) = \mathrm{ggT}(295, 187)$$
$$= \mathrm{ggT}(187, 118) = \mathrm{ggT}(118, 59) = 59.$$

Damit haben wir den Faktor 59 gefunden.

Bemerkungen

- Die benötigten Berechnungen sind für ein Rechner nicht schwierig.
- Schafft man es mit einem s nicht, einen Faktor von n zu finden, so könnte man es mit einem größeren s versuchen.
- Man könnte, wenn man bei einer elliptischen Kurve keinen Erfolg hat, einfach andere elliptische Kurven probieren. Also ist *Parallelisierung* der Berechnungen möglich.
- Es ist mit dieser Methode und heutigen Computern möglich, Primfaktoren van ca. 20-30 Dezimalstellen zu finden.

Wer Näheres zu diesem Thema (bzw. zum Inhalt der Fußnote auf der ersten Seite: siehe [1]!) wissen möchte, schlägt in den unten angeführten Büchern nach!

Wien, im Mai 2008. Dr. R. RESEL, e. h.

[1] BEUTELSPACHER, Albrecht (2001[3]): "In Mathe war ich immer schlecht …". Vieweg, Braunschweig.

[2] BEUTELSPACHER, Albrecht et al. (2005): Kryptografie in Theorie und Praxis. Vieweg, Braunschweig.

[3] WERNER, Annette (2002): Elliptische Kurven in der Kryptographie. Springer, Berlin.

Ferner zu empfehlen: Die deutschsprachige(!)[2] mathematische Zeitschrift MONOID, welche besonders für junge an der Mathematik interessierte Menschen eine geeignete Fundgrube ist und aus deren 76. Ausgabe der Artikel von de Jong stammt.

---

[2]: Es erübrigt sich (beinahe!) zu erwähnen, dass die meisten mathematischen Zeitschriften in englischer Sprache erscheinen!