Kapitel 3
Faktorisierung von Polynomen

Die Lösung sowohl einzelner Polynomgleichungen als auch von Systemen solcher Gleichungen wird mit steigendem Grad der Polynome sehr schnell sehr viel schwieriger; falls man einzelne der Polynome in Faktoren zerlegen kann, ist es meist effizienten, mit diesen zu arbeiten – obwohl die Anzahl der betrachteten Fälle bei Systemen von hinreichend vielen Polynomgleichungen auch da ziemlich groß werden kann.

Wie aus der Analysis I bekannt, läßt sich jedes Polynom über den reellen Zahlen in ein Produkt von Potenzen linearer und quadratischer Faktoren zerlegen; über den komplexen Zahlen reichen sogar lineare. Diese Art von Faktorisierung ist allerdings algorithmisch selbst bei Polynomen mit ganzzahligen Koeffizienten extrem aufwendigund lohnt nur in seltenen Fällen. Sinnvoll ist dagegen die Faktorisierung über Körpern wie $\mathbb{Q}$ oder endlichen Erweiterungen davon.

Wirklich effiziente direkte Algorithmen zur Faktorisierung sind allerdings nur über endlichen Körpern bekannt; deshalb wird auch hier unsere Strategie sein, daß wir wie beim ggT den Umweg über endliche Körper machen. Zunächst aber wollen wir Polynome über „beliebigen“ Körpern in einem ersten und billigen Schritt in quadratfreie Faktoren zerlegen, d.h. in Faktoren, in deren Primfaktorzerlegung kein irreduzibles Polynom mit einem Exponenten größer eins vorkommt. Alle folgenden Algorithmen werden sich nur mit quadratfreien Polynomen beschäftigen

Das Wort *beliebig* im vorigen Abschnitt ist in Anführungszeichen gesetzt, da wir natürlich nur über solchen Körpern arbeiten können, in denen wir die Grundrechenarten und den Test auf Gleichheit algorithmisch beschreiben können. Nach dem Satz von RICHARDSON sind damit beispielsweise die reellen und die komplexen Zahlen ausgeschlossen.

§1: Quadratfreie Zerlegung

Wir betrachten ein Polynom f über einem Körper k. Da der Polynomring $k[X]$ faktoriell ist, zerfällt f dort in ein Produkt aus einer Einheit $e \in k^\times$ und Potenzen irreduzibler Polynome aus $k[X]$:

$$f = e \prod_{i=1}^{r} f_i^{n_i} .$$

Falls alle $n_i = 1$ und kein zwei f_i zueinander assoziiert sind, bezeichnen wir f als quadratfrei. Ziel der quadratfreien Zerlegung ist es, ein beliebiges Polynom f in der Form

$$f = \prod_{j=1}^{s} g_j^{m_j}$$

zu schreiben, wobei die g_j zueinander teilerfremde quadratfreie Polynome sind. Vergleichen wir mit der obigen Darstellung und vernachlässigen wir für den Augenblick die Einheit u, so folgt, daß g_j das Produkt aller f_i mit $n_i = j$ ist.

a) Quadratfreie Zerlegung über den reellen Zahlen

Wenn ein Polynom $f \in \mathbb{R}[X]$ eine mehrfache Nullstelle hat, verschwindet dort auch die Ableitung f'. Allgemeiner gilt, daß für ein Polynom $h \in \mathbb{R}[X]$, dessen e-te Potenz f teilt, zumindest h^{e-1} auch die Ableitung f' teilen muß, denn ist $f = h^e g$, so ist

$$f' = eh^{e-1}h'g + h^e g' = h^{e-1}(eh'g + hg') .$$

Falls f *genau* durch h^e teilbar ist, ist auch f' genau durch h^{e-1} teilbar, denn wäre es sogar durch h^e teilbar, so wäre auch $eh^{e-1}h'g$ durch h^e teilbar, so daß h ein Teiler von g wäre.

Damit ist $\mathrm{ggT}(f, f') = \prod_{i=1}^{r} f_i^{e_i-1}$ und

$$q_1 = \frac{f}{\mathrm{ggT}(f, f')} = \prod_{i=1}^{r} f_i$$

ist das Produkt aller irreduzibler Faktoren von f. Alle irreduziblen Faktoren von f, die dort mindestens in der zweiten Potenz vorkommen, sind auch Teiler von f', also ist

$$g_1 = \frac{q_1}{\mathrm{ggT}(q_1, f')}$$

das Produkt aller irreduzibler Faktoren von f, die dort genau in der ersten Potenz vorkommen.

In $f_1 = f/q_1$ kommen alle irreduziblen Faktoren von f mit einem um eins verminderten Exponenten vor; insbesondere sind also die mit $e_i = 1$ verschwunden. Wenden wir darauf dieselbe Konstruktion an, erhalten wir die Zerlegung $\mathrm{ggT}(f_1, f_1') = \prod_{i=1}^{r} f_i^{\min(e_i-2,0)}$, und

$$q_2 = \frac{f_1}{\mathrm{ggT}(f_1, f_1')} = \prod_{i=1}^{r} f_i$$

ist das Produkt aller irreduzibler Faktoren von f_1, also das Produkt aller Faktoren von f, die mit einem Exponenten mindestens zwei vorkommen. Damit ist

$$g_2 = \frac{q_2}{\mathrm{ggT}(q_2, f_1')}$$

das Produkt aller Faktoren, die in f mit Multiplizität genau zwei vorkommen. Entsprechend lassen sich auch alle folgenden g_i konstruieren.

b) Ableitungen über einem beliebigen Körper

Auch wenn Ableitungen ursprünglich über Grenzwerte definiert sind, ist doch die Ableitung eines Polynoms rechnerisch gesehen eine rein algebraische Operation, die sich im Prinzip über jedem beliebigen Körper oder sogar Ring erklären läßt. Wir beschränken uns hier auf Polynome über einem Körper k und definieren die Ableitung eines Polynoms

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$$

als das Polynom

$$f' = n a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + a_1 \in k[X]\,.$$

Es ist klar, daß die so definierte Abbildung $k[X] \to k[X]$, die jedem Polynom $f \in k[X]$ seine Ableitung f' zuordnet, k-linear ist. Auch

die LEIBNIZsche Produktregel $(fg)' = fg' + fg'$ ist erfüllt: Wegen der Linearität der Ableitung und der Linearität beider Seiten der Formel sowohl in f als auch in g genügt es, dies für x-Potenzen nachzurechnen, und für $f = x^n, g = x^m$ ist $(fg)' = (n+m)x^{n+m-1}$ gleich

$$fg' + f'g = x^n m x^{m-1} + n x^{n-1} x^m = (m+n) x^{n+m-1}\,.$$

Damit gelten die üblichen Ableitungsregeln auch für die formale Ableitung von Polynomen aus $k[X]$.

Falls ein Polynom f durch das Quadrat q^2 eines anderen teilbar ist, gibt es ein Polynom $g \in k[X]$ mit $f = q^2 g$, und nach der Produktregel ist $f' = 2qg + q^2 g' = q(2g + qg')$, d.h. q teilt auch f' und damit den ggT von f und f'.

Ist umgekehrt ein irreduzibles Polynom $q \in k[X]$ Teiler von f, etwa $f = qh$, so ist $f' = q'h + qh'$ genau dann durch q teilbar, wenn $q'h$ durch q teilbar ist. Da q irreduzibel ist, muß dann entweder q' oder h durch q teilbar sein; da ersteres nicht möglich ist, folgt:

Lemma: Ein irreduzibles Polynom q ist genau dann ein mindestens quadratischer Faktor von f, wenn es den ggT von f und f' teilt. ∎

Genauer: Wenn q in der Primfaktorzerlegung von f in der Potenz q^e auftritt, d.h. $f = q^e g$ mit $q \nmid g$, so ist $f' = eq^{e-1} g + q^e g'$.

Über $\mathbb{R}$ würde daraus folgen, daß q^{e-1} die höchste q-Potenz ist, die f' teilt. Da wir aber über einem beliebigen Körper arbeiten, könnte es sein, daß der erste Faktor verschwindet: Dies passiert genau dann, wenn der Exponent e durch die Charakteristik p des Grundkörpers teilbar ist. In diesem Fall ist $f' = q^e g$ mindestens durch q^e teilbar. Da f genau durch q^e teilbar ist, folgt

Lemma: Ist $f = a \prod q_i^{e_i}$ mit $a \in k^\times$ die Zerlegung eines Polynoms $f \in k[X]$ in irreduzible Faktoren, so ist der ggT von f und f' gleich $\prod q_i^{d_i}$ mit $d_i = \begin{cases} e_i - 1 & \text{falls } p \nmid e_i \\ e_i & \text{falls } p \mid e_i \end{cases}$. ∎

Nach dem Lemma ist zumindest klar, daß $h_1 = f/\operatorname{ggT}(f, f')$ ein quadratfreies Polynom ist, nämlich das Produkt aller jener Primfaktoren von f, deren Exponent nicht durch p teilbar ist. In Charakteristik Null ist also $f/\operatorname{ggT}(f, f')$ einfach das Produkt der sämtlichen irreduziblen Faktoren von f. Diejenigen Faktoren, die mindestens quadratisch vorkommen, sind gleichzeitig Teiler des ggT; das Produkt g_1 der Faktoren, die genau in der ersten Potenz vorkommen, ist also $h_1/\operatorname{ggT}\big(h_1, \operatorname{ggT}(f, f')\big)$.

Falls $\operatorname{ggT}(f, f')$ kleineren Grad als f hat, können wir rekursiv weitermachen und nach derselben Methode das Produkt aller Faktoren bilden, die in $f_1 = \operatorname{ggT}(f, f')$ genau mit Exponent eins vorkommen; in f selbst sind das quadratische Faktoren. Weiter geht es mit $f_2 = \operatorname{ggT}(f_2, f_2')$, dessen Faktoren mit Exponent eins kubisch in f auftreten, *usw.*

Über einem Körper der Charakteristik Null liefert diese Vorgehensweise die gesamte quadratfreie Zerlegung; in positiver Charakteristik kann es allerdings vorkommen, daß $\operatorname{ggT}(f, f') = f$ ist. Da $\deg f' < \deg f$, ist dies genau dann der Fall, wenn $f' = 0$ ist. Dies ist in Charakteristik Null genau dann der Fall, wenn f konstant ist; in Charakteristik p verschwindet aber auch die Ableitung ex^{e-1} einer jeden x-Potenz, deren Exponent ein Vielfaches von p ist. Somit ist hier $f' = 0$ genau dann, wenn alle in f vorkommenden x-Potenzen einen durch p teilbaren Exponenten haben. Dann ist für $f \in \mathbb{F}_p[X]$

$$\begin{aligned} f &= a_{np}X^{np} + a_{(n-1)p}X^{(n-1)p} + \cdots + a_pX^p + a_0 \\ &= \big(a_{np}X^p + a_{(n-1)p}X^{(n-1)} + \cdots + a_pX + a_0\big)^p , \end{aligned}$$

da nach dem kleinen Satz von FERMAT in $\mathbb{F}_p$ jedes Element gleich seiner p-ten Potenz ist. f ist dann also die p-te Potenz eines anderen Polynoms, und wir können den Algorithmus auf dieses anwenden. Im Endergebnis müssen dann natürlich alle hier gefundenen Faktoren in die p-te Potenz gehoben werden.

In anderen Körpern der Charakteristik p ist die Situation etwas komplizierter: Dort müssen wir zunächst Elemente b_i finden mit $b_i^p = a_{ip}$; dann ist

$$f = \big(b_nX^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0\big)^p .$$

Solche Elemente müssen nicht existieren, es gibt aber eine große Klasse von Körpern, in denen sie stets existieren:

Definition: Ein Körper k der Charakteristik $p > 0$ heißt vollkommen, wenn die Abbildung $k \to k$; $x \mapsto x^p$ surjektiv ist.

Man kann zeigen, daß jeder endliche Körper vollkommen ist: Im Körper mit p^n Elementen ist $x^{p^n} = x$ für alle $x \in \mathbb{F}_{p^n}$, und damit ist x die p-te Potenz von $y = x^{p^{n-1}}$. Ein Beispiel eines nicht vollkommenen Körpers wäre $\mathbb{F}_p(X)$, wo X offensichtlich nicht als p-te Potenz eines anderen Körperelements geschrieben werden kann.

Über einem vollkommenen Körper der Charakteristik p kann man also jedes Polynom, dessen Ableitung das Nullpolynom ist, als p-te Potenz eines anderen Polynoms schreiben und so, falls man die p-ten Wurzeln auch effektiv berechnen kann, den Algorithmus zur quadratfreien Zerlegung durchführen.

§ 2: Der Berlekamp-Algorithmus

Wir gehen aus von einem *quadratfreien* Polynom über dem Körper $\mathbb{F}_p$ mit p Elementen, d.h. $f \in \mathbb{F}_p[X]$ ist ein Produkt von *verschiedenen* irreduziblen Polynomen $f_1, \ldots, f_r$. Durch quadratfreie Zerlegung läßt sich jedes Faktorisierungsproblem in $\mathbb{F}_p[X]$ auf diesen Fall zurückführen.

a) Ein erster Ansatz

Um zu sehen, wie wir die f_i bestimmen können, nehmen wir zunächst an, sie seien bereits bekannt. Wir wählen uns dann irgendwelche Zahlen $s_1, \ldots, s_r \in \mathbb{F}_p$ und suchen ein Polynom $v \in \mathbb{F}_p[X]$ mit

$$v \equiv s_i \bmod f_i \quad \text{für alle } i = 1, \ldots, r .$$

Da die f_i als verschiedene irreduzible Polynome vorausgesetzt waren, sind sie insbesondere paarweise teilerfremd; es gibt daher nach dem chinesischen Restesatz

Für ein quadratfreies Polynom $f \in \mathbb{F}_p[X]$ mit irreduziblen Faktoren $f_1, \ldots, f_r$ ist somit der Vektorraum V aller Polynome $v \in \mathbb{F}_p[X]$ mit

$v^p \equiv v \bmod f$ gleich dem Vektorraum aller Polynome, zu denen es Elemente $s_1, \ldots, s_r \in \mathbb{F}_p$ gibt, so daß $v \equiv s_i \bmod f_i$. Für $v \in V$ ist daher ggT$(v - \lambda, f)$ gleich dem Produkt aller f_i mit $s_i = \lambda$. Falls alle s_i verschieden sind, bekommen wir also alle Faktoren, indem wir ggT$(v-\lambda, f)$ für alle $\lambda \in \mathbb{F}_p$ berechnen; wenn sie nicht alle verschieden sind (etwa weil es mehr Faktoren gibt als Elemente von $\mathbb{F}_p$), haben wir zumindest eine teilweise Zerlegung und können mit einem neuen Polynom v zu anderen Werten s_i weitermachen.

Der einzige Nachteil an dieser Vorgehensweise besteht darin, daß wir f erst konstruieren können, *nachdem* wir die Faktoren f_i von f bereits kennen – genau diese Faktoren suchen wir aber gerade. Die Idee des BERLEKAMP-Algorithmus besteht darin, den Vektorraum V auf eine andere Weise zu charakterisieren, die ohne Kenntnis der f_i auskommt. Für diese Charakterisierung brauchen wir zunächst einige algebraische Vorbereitungen:

b) Der kleine Satz von Fermat

Zu jedem Ring R gibt es genau einen Homomorphismus $\varphi\colon \mathbb{Z} \to R$ von den ganzen Zahlen nach R, denn ein Homomorphismus muß die Eins auf die Eins abbilden und jede natürliche Zahl n entsprechend auf die Summe von n Einsen. Der Kern dieses Homomorphismus ist – wie jeder Kern eines Homomorphismus von Ringen – ein Ideal in $\mathbb{Z}$, also ein Hauptideal (p) mit $p \in \mathbb{N}_0$.

Definition: Die Charakteristik eines Körpers k ist jenes $p \in \mathbb{N}_0$, für das (p) der Kern des Homomorphismus $\mathbb{Z} \to k$ ist. Wir schreiben $p = \operatorname{char} k$.

Lemma: Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl.

Beweis: Angenommen, das ist nicht der Fall. Dann ist p eine zusammengesetzte Zahl, es gibt also zwei Zahlen $a, b < p$ in $\mathbb{N}$, so daß $p = ab$ ist. In k ist dann $a \cdot 1 \neq 0$ und $b \cdot 1 \neq 0$, aber das Produkt dieser beiden Zahlen ist $ab \cdot 1 = p \cdot 1 = 0$. Wegen der Nullteilerfreiheit eines Körpers ist das nicht möglich. ∎

Die Körper $\mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ haben natürlich allesamt Charakteristik Null, denn dort ist $\mathbb{Z}$ ein Teilring. Der Körper $\mathbb{F}_p$ ist schon konstruiert als Faktorring von $\mathbb{Z}$ mit (p) als Kern der Projektion $\mathbb{Z} \to \mathbb{F}_p$; somit ist $\operatorname{char} \mathbb{F}_p = p$.

Eines der wichtigsten Hilfsmittel der Algebra über Körpern positiver Charakteristik ist der FROBENIUS-Homomorphismus:

Lemma: Für einen Körper k der Charakteristik $p > 0$ ist die Abbildung $k \to k;\ \ x \mapsto x^p$ ein Homomorphismus.

Beweis: Natürlich ist in jedem Körper $(xy)^p = x^p y^p$; wir müssen uns überlegen, daß auch $(x+y)^p = x^p + y^p$ ist. Nach der binomischen Formel gilt

$$(x+y)^p = \binom{p}{0}x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \ldots + \binom{p}{1}xy^{p-1} + \binom{p}{p}y^p .$$

Dabei hat

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i-1)}{i!}$$

für $i \geq 1$ einen durch p teilbaren Zähler, während der Nenner für $i \leq p-1$ nicht durch p teilbar ist, denn eine Primzahl p kann natürlich keine natürliche Zahl echt kleiner p teilen. Somit ist $\binom{p}{i}$ für $1 \leq i \leq p-1$ durch p teilbar; der Term $\binom{p}{i}x^i y^{p-1}$ verschwindet also in $\mathbb{F}_p$ für alle i außer $i = 0$ und $i = p$. In diesen beiden Fällen ist der Binomialkoeffizient gleich eins, also ist $(x + y)^p = x^p + y^p$, wie behauptet. ∎

Der Homomorphismums $x \mapsto x^p$ heißt FROBENIUS-Homomorphismus; in den endlichen Körpern, die uns am meisten interessieren, sagt uns der folgende Satz, daß er trivial ist – was, wie wir im folgenden sehen werden, allerdings keinesfalls bedeutet, daß er uninteressant wäre:

Kleiner Satz von Fermat: *a)* Für eine ganze Zahl $x \in \mathbb{Z}$ und eine Primzahl p ist $x^p \equiv x \bmod p$. Ist p kein Teiler von x, so ist auch $x^{p-1} \equiv 1 \bmod p$.
b) Ist p eine Primzahl, so ist $x^p = x$ für alle $x \in \mathbb{F}_p$ und $x^{p-1} = 1$ für alle $x \neq 0$ aus $\mathbb{F}_p$.

Beweis: Natürlich ist $1^p = 1 \equiv 1 \bmod p$. Da nach dem vorigen Lemma $(x+1)^p \equiv x^p + 1^p \bmod p$, folgt daraus induktiv, daß $x^p \equiv x \bmod p$ für alle natürlichen Zahlen x. Für diese ist dann auch $(-x)^p = (-1)^p x^p \equiv -x \bmod p$ (man überzeuge sich davon, daß dies auch für $p = 2$ gilt!), und natürlich ist $0^p = 0$. Somit ist $x^p \equiv x \bmod p$ für alle $x \in \mathbb{Z}$. Da jeses $x \in \mathbb{F}_p$ einen Reprässentanten in $\mathbb{Z}$ hat, ist damit auch $x^p = x$ für alle $x \in \mathbb{F}_p$. Für $x \in \mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$ können wir durch x dividieren und erhalten $x^{p-1} = 1$. Für eine nicht durch p teilbare ganze Zahl x folgt, daß ihre Restklasse modulo p die Eins als $(p-1)$-te Potenz hat, also ist $x^{p-1} \equiv 1 \bmod p$. ∎

Korollar: Über einem Körper k der Charakteristik $p > 0$ ist

$$X^p - X = \prod_{i=0}^{p-1}(X - i) \quad \text{und} \quad X^{p-1} - 1 = \prod_{i=1}^{p-1}(X - i)\,.$$

Beweis: Nach dem kleinen Satz von FERMAT sind die betreffenden Elemente Nullstellen, und da ein von Null verschiedenes Polynom vom Grad n nicht mehr als n Nullstellen haben kann, gibt es keine weiteren. Die Gleichheit beider Seiten folgt somit daraus, daß die führenden Koeffizienten beider Polynome Eins sind. ∎

c) Anwendung auf den Berlekamp-Algorithmus

Sei nun wieder $f = f_1 \cdots f_r \in \mathbb{F}_p[X]$ ein quadratfreies Polynom vom Grad n mit irreduziblen Faktoren f_i. Wir betrachteten Polynome $v \in \mathbb{F}_p[X]$ vom Grad höchstens $n-1$ mit der Eigenschaft $v \equiv s_i \bmod f_i$ für irgendwelche Elemente $s_i \in \mathbb{F}_p$. Für ein solches Polynom

$$v = v_{n-1}X^{n-1} + v_{n-2}X^{n-2} + \cdots + v_1 X + v_0$$

...

d) Durchführung des Berlekamp-Algorithmus

Die zweite Charakterisierung von V zeigt, daß die Dimension von V gleich der Anzahl r der irreduziblen Faktoren von f ist; insbesondere ist also V eindimensional genau dann, wenn f irreduzibel ist.

Andernfalls wählen wir irgendein Element $v \in V$ und berechnen die Polynome $\mathrm{ggT}(v - \lambda, f)$ für alle $\lambda \in \mathbb{F}_p$. Falls wir dabei r mal ein nichtkonstantes Polynom bekommen, haben wir f faktorisiert. Wenn wir zu wenige Faktoren bekommen, waren für das betrachtete Polynom v einige der Werte s_i gleich; wir bilden eine Liste der gefundenen (und zumindest noch nicht in allen Fällen irreduziblen) Faktoren und wählen wir ein von v linear unabhängiges neues Polynom $w \in V$ und machen damit dasselbe. Indem wir für jedes nichtkonstante Polynom $\mathrm{ggT}(w - \lambda, f)$ den ggT mit den in der Liste stehenden Faktoren bilden, können wir die Listenelemente weiter zerlegen. Bei jeder gefundenen Zerlegung ersetzen wir das zerlegte Element durch seine Faktoren. Sobald die Liste r Faktoren enthält, sind wir fertig.

Falls die sämtlichen $\mathrm{ggT}(w - \lambda, f)$ immer noch nicht ausreichen, um r Faktoren zu produzieren, müssen wir ein neues, von v und w linear unabhängiges Element von V wählen und damit weitermachen, *usw.*

Das Verfahren muß spätestens mit dem r-ten Polynom v enden, denn dann haben wir eine Basis $v_1, \ldots, v_n$ von V durchprobiert. Hätten wir dann noch nicht alle r Faktoren isoliert, müßte es (mindestens) zwei Faktoren f_i und f_j geben, so daß $v_\ell \bmod f_i = v_\ell \bmod f_j$ ist für alle Basiselemente v_ℓ und damit auch $v \bmod f_i = v \bmod f_j$ für alle $v \in V$. Das ist aber nicht möglich, denn nach dem chinesischen Restesatz enthält V beispielsweise auch ein Element v mit $v \bmod f_i = 0$ und $v \bmod f_j = 1$.

§3: Faktorisierung über den ganzen Zahlen und über endlichen Körpern

Wie bei der Berechnung des ggT zweier Polynome wollen wir auch bei der Faktorisierung den Umweg über endliche Körper benutzen, um Probleme für Polynome über $\mathbb{Z}$ zu lösen. Allerdings kann es hier häufiger passieren, daß sich Ergebnisse über $\mathbb{F}_p$ deutlich unterscheiden von denen über Z.

Betrachten wir dazu als erstes Beispiel das Polynom $X^2 + 1$ aus $\mathbb{Z}[X]$. Es ist irreduzibel, da eine Zerlegung die Form $(X - a)(X + a)$ haben müßte mit $a \in \mathbb{Z}$, und in Z gibt es kein Element a mit $a^2 = -1$.

Auch über dem Körper $\mathbb{F}_p$ muß eine eventuelle Faktorisierung die Form $(X-a)(X+a)$ haben mit $a^2=-1$; wir müssen uns also überlegen, wann das der Fall ist. Die elementare Zahlentheorie sagt uns:

Lemma: Genau dann gibt es im endlichen Körper $\mathbb{F}_p$ ein Element a mit $a^2=-1$, wenn $p=2$ oder $p\equiv 1 \bmod 4$ ist.

Beweis: Für $p=2$ ist natürlich $1^2=1=-1$ die Lösung. Für $p\equiv 1 \bmod 4$ schreiben wir $p=4k+1$. Nach dem kleinen Satz von FERMAT ist für alle $x\in\mathbb{F}_p^\times$

$$(x^{p-1}-1)=(x^{2k}+1)(x^{2k}-1)=0\,,$$

das linksstehende Polynom hat also $p-1=4k$ Nullstellen und zerfällt damit über $\mathbb{F}_p$ in Linearfaktoren. Damit gilt dasselbe für die beiden rechtsstehenden Faktoren; insbesondere gibt es also ein $x\in\mathbb{F}_p$ mit $x^{2k}+1=0$. Für $a=x^k$ ist dann $a^2=x^{2k}=-1$.

Ist $p\equiv 3 \bmod 4$ und $a^2=-1$ für ein $a\in\mathbb{F}_p$, so ist $a^4=1$. Außerdem ist nach dem kleinen Satz von FERMAT $a^{p-1}=1$. Da $p\equiv 3 \bmod 4$ ist $\mathrm{ggT}(4,p-1)=2$ als Linearkombination von 2 und $p-1$ darstellar, also ist auch $a^2=1$, im Widerspruch zu Annahme $a^2=-1$. Somit gibt es in $\mathbb{F}_p$ keine Elemente mit Quadrat -1. ∎

Damit ist X^2+1 genau dann irreduzibel über $\mathbb{F}_p$, wenn $p\equiv 3 \bmod 4$; in allen anderen Fällen zerfällt das Polynom in zwei Linearfaktoren. Nach DIRICHLETs Satz über Primzahlen in arithmetischen Progressionen bleibt X^2+1 damit nur modulo der Hälfte aller Primzahlen irreduzibel.

Noch schlimmer ist es bei X^4+1: Auch dieses Polynom ist irreduzibel über $\mathbb{Z}$: Da seine Nullstellen $\frac{1}{2}\sqrt{2}(\pm 1\pm i)$ nicht in $\mathbb{Z}$ liegen, gibt es keinen linearen Faktor, und wäre

$$\begin{aligned}X^4+1&=(X^2+aX+b)(X^2+cX+d)\\&=X^4+(a+c)X^3+(b+d+ac)X^2+(ad+bc)X+bd\end{aligned}$$

eine Zerlegung in quadratische Faktoren, so zeigen die Koeffizieten von X^3 und der konstante Term, daß $c=-a$ und $b=d=\pm 1$ sein

müßte. Die Produkte

$$(X^2+aX+1)(X^2-aX+1)=X^4+(2-a^2)X^2+1$$

und

$$(X^2+aX-1)(X^2-aX-1)=X^4-(2+a^2)X^2+1$$

zeigen aber, daß beides nur für $a^2=\pm 2$ zu einer Faktorisierung führen könnte, was in $\mathbb{Z}$ nicht erfüllbar ist.

In den Körpern $\mathbb{F}_p$ dagegen kann es sehr wohl Elemente geben, deren Quadrat ± 2 ist, und dann zeigen die obigen Formeln, daß X^4+1 dort in ein Produkt zweier quadratischer Polynome zerlegt werden kann. Auch wenn es ein Element $a\in\mathbb{F}_p$ gibt mit $a^2=-1$, können wir X^4+1 als Produkt schreiben, nämlich genau wie oben im Falle X^2+1 als

$$X^4+1=(X^2+a)(X^2-a)\,.$$

Somit ist X^4+1 über dem Körper $\mathbb{F}_p$ zumindest dann reduzibel, wenn dort wenigstens eines der drei Elemente -1 und ± 2 ein Quadrat ist. Um zu sehen, daß X^4+1 über jedem dieser Körper zerfällt, müssen wir uns also überlegen, daß in keinem der Körper $\mathbb{F}_p$ alle drei Elemente *keine* Quadrate sind. Da $-2=-1\cdot 2$ ist, folgt dies aus

Lemma: Sind im Körper $\mathbb{F}_p$ die beiden Elemente a,b nicht als Quadrate darstellbar, so ist ab ein Quadrat.

Beweis: Für $p=2$ ist jedes Element ein Quadrat und nicht zu beweisen. Ansonsten betrachten wir die Abbildung $\mathbb{F}_p^\times\to\mathbb{F}_p^\times$, die jedes von Null verschiedene Element von $\mathbb{F}_p$ auf sein Quadrat abbildet. Sie ist offensichtlich ein Homomorphismus von multiplikativen Gruppen, und da $1\neq p-1=-1$ ist, besteht ihr Kern aus genau zwei Elementen. Nach dem Homomorphiesatz hat das Bild somit $\frac{1}{2}(p-1)$ Elemente, d.h. die Hälfte alle Elemente von $\mathbb{F}_p^\times$ sind Quadrate. Ist a keines, so ist auch ax^2 für kein $x\in\mathbb{F}_p^\times$ ein Quadrat y, denn sonst wäre $a=(y^2x^{-2}$ selbst ein Quadrat.

Da es $\frac{1}{2}(p-1)$ Quadrate und genauso viele Nichtquadrate gibt, läßt sich somit jedes Nichtquadrat b als $b = ax^2$ schreiben mit einem geeigneten Element $x \in \mathbb{F}_p$. Damit ist $ab = (ax)^2$ ein Quadrat.

∎

Die Situation kann hier also deutlich schlechter werden als im Fall des EUKLIDischen Algorithmus, wo wir sicher sein konnten, daß es höchstens endlich viele schlechte Primzahlen gibt: Hier können *alle* Primzahlen schlecht sein in dem Sinne, daß ein irreduzibles Polynom aus $\mathbb{Z}[X]$ modulo p reduzibel wird, und oft wird zumindest die Hälfte aller Primzahlen schlecht sein. Der Ansatz über den chinesischen Restesatz empfiehlt sich hier also definitiv nicht: Wenn wir die Faktorisierung modulo verschiedener Primzahlen durchführen, können wir praktisch sicher sein, daß es darunter auch schlechte gibt, und meist werden auch die Ergebnisse modulo verschiedener Primzahlen entweder nicht zusammenpassen, oder aber wir haben mehrere Faktoren gleichen Grades, von denen wir nicht wissen, welche wir via chinesischen Restesatz miteinander kombinieren sollen. Es hat daher keinen Zweck, zufällig Primzahlen zu wählen und dann eine Rückfallstrategie für schlechte Primzahlen

Der Weg über endliche Körper verfolgt daher im Falle der Faktorisierung eine andere Strategie als beim EUKLIDischen Algorithmus: Wir beschränken uns auf eine einzige Primzahl – unabhängig davon, ob diese nun gut oder schlecht dafür geeignet ist.

Wir kennen bereits aus dem Kapitel über den EUKLIDischen Algorithmus Schranken für die Koeffizienten der Faktoren eines Polynoms; wir könnten also eine Primzahl wählen, die größer ist als das Doppelte dieser Schranke und modulo dieser rechnen.

Der Nachteil dabei ist, daß das Rechnen modulo einer Primzahl p umso teurer wird, je größer die Primzahl ist: Die Kosten für Multiplikationen wachsen quadratisch mit der Stellenzahl von p, die Kosten für Divisionen modulo p nach dem erweiterten EUKLIDischen Algorithmus können sogar bis zu kubisch ansteigen.

Die Alternative bietet ein für völlig andere Zwecke bewiesenes Resultat des deutschen Zahlentheoretikers HENSEL, das es erlaubt eine Faktorisierung modulo p fortzusetzen zu einer Faktorisierung modulo jeder

beliebiger p-Potenz und, was HENSEL wirklich interessierte, zu den p-adischen Zahlen, mit denen wir uns in Rahmen dieser Vorlesung nicht beschäftigen werden.

§4: Das Henselsche Lemma

Lemma: f, g, h seien Polynome aus $\mathbb{Z}[X]$ derart, daß $f \equiv gh \bmod p$; dabei seien $g \bmod p$ und $h \bmod p$ teilerfremd über $\mathbb{F}_p[X]$. Dann gibt es für jede natürliche Zahl n Polynome g_n, h_n derart, daß

$$g_n \equiv g \bmod p, \quad h_n \equiv hh \bmod p \quad \text{und} \quad f \equiv g_n h_n \bmod p^n .$$

Beweis durch vollständige Induktion: Der Fall $n = 1$ ist die Voraussetzung des Lemmas. Ist das Lemma für ein n bewiesen, machen wir den Ansatz

$$g_{n+1} = g_n + p^n g^* \quad \text{und} \quad h_{n+1} = h_n + p^n h^* .$$

Nach Induktionsvoraussetzung ist $f \equiv g_n h_n \bmod p^n$, die Differenz $f - g_n h_n$ ist also durch p^n teilbar und es gibt ein Polynom $f^* \in \mathbb{Z}[X]$, so daß $f = g_n h_n + p^n f^*$ ist. Wir möchten, daß

$$f \equiv (g_n + p^n g^*)(h_n + p^n h^*) = g_n h_n + p^n (g_n h^* + h_n g^*) + p^{2n} \bmod p^{n+1}$$

ist. Da $2n \geq n + 1$ ist, können wir den letzten Summanden vergessen; zu lösen ist also die Kongruenz

$$f \equiv g_n h_n + p^n f^* = g_n h_n + p^n (g_n h^* + h_n g^*) \bmod p^{n+1}$$

oder

$$p^n f^* \equiv p^n (g_n h^* + h_n g^*) \bmod p^{n-1} .$$

Division durch p^n macht daraus

$$f^* \equiv g_n h^* + h_n g^* \bmod p \quad \text{oder} \quad f^* \equiv gh^* + hg^* \bmod p ,$$

denn $g_n \equiv g \bmod p$ und $h_n \equiv h \bmod p$. Die letztere Kongruenz können wir als Gleichung in $\mathbb{F}_p[X]$ auffassen und dort lösen, indem wir den erweiterten EUKLIDischen Algorithmus auf die Polynome $g \bmod p$ und $h \bmod p$ aus $\mathbb{F}_p[X]$ anwenden: Da diese nach Voraussetzung teilerfremd sind, können wir ihren ggT Eins und damit auch jedes andere Polynom

über $\mathbb{F}_p$ als Linearkombination der beiden darstellen. Da der Grad von f die Summe der Grade von g und h ist und f^* höchstens denselben Grad wie f hat, können wir dann auch eine Darstellung $f^* = gh^* + hg^*$ in $\mathbb{F}_p[X]$ finden mit $\deg g^* \leq \deg g$ und $\deg h^* \leq \deg h$. Ersetzen wir g^* und h^* durch irgendwelche Repräsentantanten gleichen Grades aus $\mathbb{Z}[X]$ erfüllen dann $g_{n+1} = g_n + p^n g^*$ und $h_{n+1} = h_n + p^n h^*$ die Kongruenz $f \equiv g_n h_n$ modulo p^{n+1}.

■

§5: Der Algorithmus von Zassenhaus

Die Werkzeuge aus den vorigen Paragraphen erlauben, gemeinsam eingesetzt, nun die Faktorisierung von Polynomen über $\mathbb{Z}$. Nach ZASSENHAUS geht man dabei folgendermaßen vor:

Erster Schritt: Auch wenn es nicht unbedingt nötig ist, sollte man beginnen mit einer quadratfreien Zerlegung des Polynoms $f \in \mathbb{Z}[X]$ oder besser seines primitiven Anteils über $\mathbb{Q}[X]$; die primitiven Anteile davon liefern dann eine quadratfreie Zerlegung über $\mathbb{Z}[X]$, und auf diese quadratfreie Faktoren werden die folgenden Schritte angewendet.

Zweiter Schritt: Berechne eine obere Schranke L für die Koeffizienten der Faktoren des Polynoms und setze $M = 2L + 1$. Wähle eine Primzahl p, die den führenden Koeffizienten nicht teilt und führe eine quadratfreie Zerlegung über $\mathbb{F}_p$ durch. (Dies ist trotz des ersten Schritts notwendig, denn ein in $\mathbb{Z}[X]$ quadratfreies Polynom muß keine quadratfreie Reduktion in $\mathbb{F}_p[X]$ haben.) Wende die folgenden Schritte an für jeden der quadratfreien Faktoren.

Dritter Schritt: Faktorisiere das Polynom nach BERLEKAMP in $\mathbb{F}_p[X]$.

Vierter Schritt: Hebe die Faktorisierung nach dem HENSELschen Lemma hoch zu einer Faktorisierung modulo p^n für eine natürliche Zahl n derart, daß $p^n \geq M$ ist.

Fünfter Schritt: Setze $m = 1$ und teste für jeden der gefundenen Faktoren, ob er das zu faktorisierende Polynom teilt. Falls ja, kommt der Faktor in die Liste L_1 der Faktoren von f; andernfalls kommt es in eine Liste L_2.

Sechster Schritt: Falls die Liste L_2 keine Einträge hat, endet der Algorithmus und f ist das Produkt der Faktoren aus L_1. Andernfalls setze $m = m + 1$ und teste für jedes Produkt aus m verschiedenen Polynomen aus L_2, ob ihr Produkt modulo p^n (mit Koeffizienten vom Betrag höchstens L) ein Teiler von f ist. Falls ja, entferne man die m Faktoren aus L_1 und füge ihr Produkt in die Liste L_1 ein. Wiederhole diesen Schritt.

Auch wenn der sechste Schritt wie eine Endlosschleife aussieht, endet der Algorithmus natürlich nach endlich vielen Schritten, denn L_2 ist eine endliche Liste und spätestens das Produkt aller Elemente aus L_2 muß Teiler von f sein, da sein Produkt mit dem Produkt aller Elemente von L_1 gleich f ist.

§6: Ausblicke

Der sechste Schritt des obigen Algorithmus kann sehr teuer werden, insbesondere wenn man auch Produkte von mehr als zwei Faktoren testen muß. Es gibt einen Algorithmus von LENSTRA, LOVACZ und LENSTRA, den sogenannten LLL-Algorithmus, mit dem man auf systematischere Weise geeignete Kandidaten für zu testende Produkte finden kann. Für Einzelheiten fehlt hier leider die Zeit; man findet sie aber in praktisch jedem neueren Lehrbuch der Computeralgebra oder der algorithmischen Zahlentheorie. LLL findet ganz allgemein kürzeste Vektoren in Gittern der Form $\bigoplus_{i=1}^{m} \mathbb{Z}\vec{v}_i \subset \mathbb{R}^n$ und hat daher noch zahlreiche weitere Anwendungen abgesehen von der Faktorisierung.

Mit nur geringfügiger Modifikation kann der obige Algorithmus auch zur Faktorisierung von Polynomen in mehr als einer Veränderlichen benutzt werden. Auch hier wird das Problem zurückgeführt auf den BERLEKAMP-Algorithmus in $\mathbb{F}_p[X]$, und zwar indem man alle Variablen mit einer Ausnahme auf spezielle Werte setzt. Auch für Faktorisierungen modulo einem Polynom $(X_i - a_i)$ gibt es ein HENSELsches Lemma, mit dem man diese hochheben kann zu Faktorisierungen modulo $(X_i - a_i)^r$, wobei man für r mindestens den Grad von f in X_i wählen muß. Wie oben ist der sechste Schritt oft der umfangreichste; im Gegensatz zur

Situation über $\mathbb{Z}[X]$ gibt es jedoch keinen LLL-Algorithmus, um diesen Schritt zu beschleunigen. Für Einzelheiten sei auf die Originalarbeiten verwiesen, z.B.

P.S. WANG: An improved multivariable polynomial factorising algorithm, *Mathematics of Computation* **32** (1978), 1215-1231