ggT-Berechnung über das Henselsche Lemma

Das HENSELsche Lemma gestattet es, eine Faktorisierung in zwei zueinander teilerfremde Faktoren modulo einer Primzahl p hochzuheben zu einer Faktorisierung modulo einer beliebigen Potenz p^n dieser Primzahl. In der Computeralgebra nutzte das als erster HANS JULIUS ZASSENHAUS (1912–1991), einer der Pioniere der Computeralgebra, aus um 1969 einen Algorithmus zur Faktorisierung von Polynomen aufzustellen. Vier Jahre später griffen JOEL MOSES und DAVID Y. Y. YUN diese Idee auf, um eine neue modulare Methode zur ggT-Berechnung vorzuschlagen; sie bezeichneten sie als EZ GCD Algorithm für *Extended Zassenhaus Greatest Common Divisor.*

Die Grundidee ist einfach: Für zwei primitive Polynome $f, g \in \mathbb{Z}[X]$ wählt man eine zufällige Primzahl p, die nicht beide führende Koeffizienten teilt, und berechnet nach dem EUKLIDischen Algorithmus den ggT von $f \bmod p$ und $g \bmod p$; das Polynom $h \in \mathbb{Z}[X]$ sei modulo p gleich diesem ggT. Dazu bestimmt man Polynome $f^*, g^* \in \mathbb{Z}[X]$, die modulo p gleich den Quotienten $(f \bmod p)/h$ und $(g \bmod p)/h$ sind; in $\mathbb{Z}[X]$ ist also

$$f \equiv h \cdot f^* \bmod p \quad \text{und} \quad g = h \cdot g^* \bmod p\,.$$

Falls h und f^* oder h und g^* zueinander teilerfremd sind, kann man die entsprechende Faktorisierung nach dem HENSELschen Lemma hochheben zu einer Faktorisierung von f oder g modulo einer beliebig großen Potenz von p. Sobald diese Potenz p^n größer ist als das Doppelte der LANDAU-MIGNOTTE-Schranke, ersetzt man h gegebenenfalls durch ein modulo p^n dazu kongruentes Polynom, dessen Koeffizienten einen Betrag höchstens gleich dieser Schranke haben. Falls das nicht möglich ist, wissen wir wieder, daß der ggT der Polynome modulo p einen größeren Grad hat als der ggT der Ausgangspolynome, so daß wir den Algorithmus mit einer neuen Primzahl wiederholen müssen. Andernfalls müssen wir noch testen, ob das so konstruierte Polynom sowohl f als auch g teilt; wenn ja, haben wir den ggT gefunden, wenn nein, müssen wir mit einer neuen Primzahl noch einmal von vorne anfangen.

Man beachte, daß es durchaus vorkommen kann, daß weder h und f^*

noch h und g^* teilerfremd sind: Die beiden Polynome

$$f = (X-1)^2(X-2)(X-3) \quad \text{und} \quad g = (X-1)(X-2)^2(X-4)$$

etwa haben den ggT $h = (X-1)(X-2)$. Somit ist $f = h\cdot(X-1)(X-3)$ und $g = h\cdot(X-2)(X-4)$, und in beiden Fällen hat der Kofaktor einen gemeinsamen Teiler mit h.

In solchen Fällen hilft ein Trick von DAVID SPEAR: Für jedes Paar (a,b) ganzer Zahlen mit $b \neq 0$ ist $\mathrm{ggT}(f,g) = \mathrm{ggT}(f, af+bg)$. Ist nun $h \equiv \mathrm{ggT}(f \bmod p, g \bmod p) \bmod p$ und $f \equiv h\cdot f^* \bmod p$ sowie $g \equiv h\cdot g^* \bmod p$, so ist $af+bg \equiv h\cdot(af^*+bg^*) \bmod p$, und da $f^* \bmod p$ und $g^* \bmod p$ teilerfremd sind, gibt es unendlich viele Paare (a,b), für die $af^* + bg^*$ teilerfremd ist zu h. Man wählt also so lange zufällig ein Paar (a,b) bis $af^* + bg^*$ teilerfremd zu h ist. Danach kann man nach dem HENSELschen Lemma die Faktorisierung $af+bg \equiv h\cdot(af^*+bg^*)$ hochheben und weiter vorgehen wie oben. Im obigen Beispiel etwa ist $f^* = (X-1)(X-3)$ und $g^* = (X-2)(X-4)$; das Polynom f^*+g^* hat für $X = 1$ den Wert drei und für $X = 2$ den Wert -1, ist also teilerfremd zu $h = (X-1)(X-2)$, so daß wir hier $a = b = 1$ wählen könnten.

Wenn wir ausmultiplizieren, erhalten wir in diesem Beispiel

$$f = X^4-7X^3+17X^2-17X+6 \quad \text{und} \quad g = X^4-9X^3+28X^2-36X+16\,;$$

die LANDAU-MIGNOTTE-Schranke liegt knapp unter 412,3. Wir wählen die Primzahl $p = 101$ und erhalten

$$\mathrm{ggT}(f \bmod 101, g \bmod 101) = X^2 + 98X + 2\,.$$

Dividieren wir f und g modulo 101 durch dieses Polynom, erhalten wir

$$f \equiv (X^2+98X+2)(X^2+97X+3) \bmod 101$$

und

$$g \equiv (X^2+98X+2)(X^2+95X+8) \bmod 101\,;$$

Anwendung des EUKLIDischen Algorithmus in $\mathbb{F}_{101}[X]$ zeigt, daß

$$\mathrm{ggT}(X^2+98X+2, X^2+97X+3) = X+100$$

und

$$\mathrm{ggT}(X^2+98X+2, X^2+95X+8) = 3X+95$$

ist. Somit haben wir in keinem der beiden Fälle einen zu h teilerfremden Kofaktor und probieren es mit einer Linearkombination:

$$f + g = 2X^4 - 16X^3 + 45X^2 - 53X + 22 \equiv h \cdot (2X^2 + 91X + 11)\,,$$

und $q = 2X^2 + 91X + 11$ ist teilerfremd zu h. Genauer zeigt eine Anwendung des erweiterten EUKLIDischen Algorithmus in $\mathbb{F}_{101}[X]$, daß

$$(70X + 25)h + (66X + 69)q \equiv 1 \bmod 101$$

ist.

Zur Anwendung des HENSELschen Lemmas machen nun den Ansatz

$$f + g \equiv (h + 101h^*)(q + 101q^*) \equiv hq + 101(hq^* + h^*q) \bmod 101^2\,.$$

$hq = 2X^4 + 287X^3 + 8933X^2 + 1260X + 22$ ist kongruent zu $f + g$ modulo 101, und

$$\frac{f + g - hq}{101} = -3X^3 - 88X^2 - 13X\,.$$

Wir müssen also Polynome q^* und h^* finden, so daß $hq^* + h^*q$ modulo 101 gleich diesem Polynom ist. Die obige Darstellung der Eins als Linearkombination von h und q führt auf

$$\begin{aligned}(70X+25)(-3X^3-88X^2-13X)h+(66X+69)(-3X^3-88X^2-13X)q\\ \equiv -3X^3 - 88X^2 - 13X) \bmod 101\,;\end{aligned}$$

ausmultipliziert modulo 101 wird das zu

$$\begin{aligned}(93X^4 + 27X^3 + 21X^2 + 19X)h + (4X^4 + 25X^3 + 39X^2 + 12X)q\\ \equiv -3X^3 - 88X^2 - 13X \bmod 101\,.\end{aligned}$$

Die Vorfaktoren von h und q haben hier natürlich noch einen viel zu hohen Grad; da wir beliebige Vielfache der Gleichung $qh - hq = 0$ subtrahieren dürfen, können wir den Faktor vor h ersetzen durch seinen Rest bei der Division durch q, und den vor q durch seinen Rest bei der Division durch h, wobei wir natürlich alle Divisionen in $\mathbb{F}_{101}[X]$ ausführen müssen. Beide Reste sind gleich $100x$; wir erhalten also die erheblich einfachere Kongruenz

$$100Xh + 100Xq \equiv -3X^3 - 88X^2 - 13X \bmod 101\,.$$

Somit können wir $q^* = h^* = 100X$ setzen und erhalten die Kongruenz

$$\begin{aligned} f + q &\equiv (h + 101h^*)(q + 101q^*) \\ &= (X^2 + 10198X + 2)(X^2 + 10191X + 11) \bmod 101^2 . \end{aligned}$$

101^2 liegt über dem Doppelten der LANDAU-MIGNOTTE-Schranke; da $10198 \equiv -3 \bmod 101^2$, ist $X^2 - 3X + 2$ ein Polynom aus $\mathbb{Z}[X]$, das modulo 101^2 kongruent zum ersten Faktor ist und Koeffizienten vom Betrag unterhalb der LANDAU-MIGNOTTE-Schranke hat und somit ein Kandidat für den ggT ist. Tatsächlich zeigt Polynomdivision in $\mathbb{Z}[X]$, daß dieses Polynom sowohl f als auch g teilt und damit gleich dem größten gemeinsamen Teiler dieser beiden Polynome ist.

(Wenn wir die Restklassen modulo 101 nicht durch die Zahlen von Null bis hundert repräsentiert hätten, sondern durch die zwischen -50 und 50, hätten wir schon modulo 101 den ggT $X^2 - 3X + 2$ erhalten und hätten bei der Division in $\mathbb{F}_{101}[X]$ gesehen, daß dieses Polynom bereits in $\mathbb{Z}[X]$ Teiler sowohl von f als auch von g ist. Da 101 keinen führenden Koeffizienten teilt und der modulare ggT mindestens den Grad des ggT in $\mathbb{Z}[X]$ hat, hätten wir bereits an dieser Stelle erkannt, daß dies der ggT sein muß.)

Im vorliegenden Beispiel mußten wir eines der zu faktorisierenden Polynome durch eine Linearkombination der beiden Polynome ersetzten, da wir das HENSELsche Lemma nur auf Produkte von teilerfremden Polynomen anwenden können. Alternativ hätten wir auch durch eine Vorverarbeitung der beiden Polynome sicherstellen können, daß der Kofaktor jeweils teilerfremd zum ggT ist: Jedes Polynom f läßt sich bekanntlich zerlegen in ein Produkt $f = q_1^{e_1} \cdots q_r^{e_r}$ von Potenzen irreduzibler Polynome q_i, wobei wir annehmen können, daß es keine Indizes $i \neq j$ gibt, für die q_j gleich einer Einheit mal q_i ist. Falls in dieser Zerlegung alle Exponenten gleich eins sind, bezeichnen wir das Polynom als *quadratfrei,* und in diesem Fall sind offensichtlich bei jeder Produktzerlegung $f = gh$ die beiden Faktoren g und h teilerfremd. Während die vollständige Faktorisierung eines Polynoms recht aufwendig ist, läßt sich eine sogenannte *quadratfreie Zerlegung* recht einfach mit Hilfe des EUKLIDischen Algorithmus konstruieren. Bei dieser Zerlegung wird f dargestellt in der Form $f = g_1 \cdot g_2^2 \cdots g_s^s$,

wobei jedes der Polynome g_j quadratfrei ist. Wenn wir mit der obigen Zerlegung vergleichen, ist g_j offensichtlich das Produkt aller q_i, die mit Exponent $e_i = j$ auftreten

Wir betrachten zunächst ein Polynom f über einem Körper, der dies rationalen Zahlen enthält; seine Zerlegung in irreduzible Faktoren sei $f = q_1^{e_1} \cdots q_r^{e_r}$. Dann ist die (formale) Ableitung f' von f für jedes i durch $q_i^{e_i-1}$ teilbar, nicht aber durch $q_i^{e_i}$. Somit ist

$$\mathrm{ggT}(f, f') = q_1^{e_1-1} \cdots q_r^{e_r-1} \quad \text{und} \quad h_1 = \frac{f}{\mathrm{ggT}(f, f')} = q_1 \cdots q_r$$

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

$$g_1 = \frac{h_1}{\mathrm{ggT}(h_1, f')}$$

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

In $f_1 = f/h_1$ 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 $\mathrm{ggT}(f_1, f_1') = \prod_{i=1}^{r} q_i^{\max(e_i-2,0)}$, und

$$h_2 = \frac{f_1}{\mathrm{ggT}(f_1, f_1')} = \prod_{i=1}^{r} q_i$$

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

$$g_2 = \frac{h_2}{\mathrm{ggT}(h_2, f_1')}$$

das Produkt aller Faktoren, die in f mit Multiplizität genau zwei vorkommen.

Nach dem gleichen Schema können wir, falls $f_2(x)$ nicht konstant ist, weitermachen und rekursiv für $j \geq 3$ definieren

$$h_j = \frac{f_{j-1}}{\mathrm{ggT}(f_{j-1}, f_{j-1}'}, \quad g_j(x) = \frac{h_j}{\mathrm{ggT}(h_j, f_{j-1}')} \quad \text{und} \quad f_j(x) = \frac{f_{j-1}}{h_i},$$

bis wir für ein konstantes f_j erhalten. Dann hat keines der Polynome g_j mehrfache Faktoren, oder jeder irreduzible Faktor vonÂflg_j kommt in der Zerlegung von f mit Exponent j vor.

Bis auf eine eventuell notwendige Konstante c ist damit f das Produkt der Polynome g_j^j, und alle g_j sind quadratfrei.

Als Beispiel betrachten wir das Polynom

$$f(x) = X^4 - 5X^2 + 6X - 2 \quad \text{mit} \quad f'(X) = 4X^3 - 10X + 6\,.$$

Wir berechnen zunächst den ggT von f und f':

$$(X^4 - 5X^2 + 6X - 2) : (4X^3 - 10X + 6) = \frac{X}{4} \text{ Rest } -\frac{5}{2}X^2 + \frac{9}{2}X - 2$$

$$(4X^3 - 10X + 6) : \left(-\frac{5}{2}X^2 + \frac{9}{2}X - 2\right) = -\frac{8}{5}X - \frac{72}{25} \text{ Rest } -\frac{6}{25}X + \frac{6}{25}$$

$$\left(-\frac{5}{2}X^2 + \frac{9}{2}X - 2\right) : \left(-\frac{6}{25}X + \frac{6}{25}\right) = \frac{125}{12}X - \frac{25}{3}$$

Somit ist der ggT gleich $-\frac{6}{25}(X - 1)$; da es auf Konstanten nicht ankommt, rechnen wir besser mit $(X - 1)$.

Eigentlich sind wir damit schon fertig: Der ggT hat nur die einfache Nullstelle $x = 1$, also hat $f(x)$ an der Stelle eins eine doppelte Nullstelle, und alles andere sind einfache Nullstellen. Da

$$(X^4 - 5X^2 + 6X - 2) : (X - 1)^2 = X^2 + 2X - 2$$

ist, haben wir die quadratfreie Zerlegung

$$f(X) = (X^2 + 2X - 2) \cdot (X - 1)^2\,.$$

Zur Illustration können wir aber auch strikt nach Schema weiterrechnen. Dann brauchen wir als nächstes

$$h_1 = \frac{f}{\text{ggT}(f, f')} = \frac{X^4 - 5X^2 + 6X - 2}{X - 1} = X^3 + X^2 - 4X + 2\,,$$

das Polynom das an jeder Nullstelle von $f(X)$ eine einfache Nullstelle hat. Sodann brauchen wir den ggT von $h_1(X)$ und $f'(X)$; da wir schon

wissen, daß f und f' außer der Eins keine gemeinsame Nullstelle haben, muß das $(X-1)$ sein. Somit ist

$$g_1 = \frac{X^3+X^2-4X+2}{X-1} = X^2+2X-2 = (X+1)^2-3$$

das Polynom, das genau bei den einfachen Nullstellen von f verschwindet, also bei $-1\pm\sqrt{3}$. Als nächstes muß

$$g_1(X) = \frac{f(X)}{h_1(X)} = \frac{X^4-5X^2+6X-2}{X^3+X^2-4X+2} = X-1$$

untersucht werden; da es nur für $X=1$ verschwindet, ist die Eins eine doppelte Nullstelle von f. Damit sind alle Nullstellen von $f(X)$ sowie auch deren Vielfachheiten gefunden.

Wenn der Körper k die rationalen Zahlen nicht enthält, funktioniert der beschriebene Algorithmus eventuell nicht: Wenn wir etwa über dem Körper $\mathbb{F}_3$ das Polynom $f = 2X^9+X^6+X^3+2$ betrachten, so ist $f' = 18X^8+6X^5+3X^2 = 0$, da alle Koeffizienten durch drei teilbar sind und somit in $\mathbb{F}_3$ verschwinden. Daher muß der Algorithmus für solche Körper etwas modifiziert werden. Nach dem binomischen Lehrsatz ist

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

mit $\binom{n}{i} = \frac{n!}{i!(n-i)!}$. Für eine Primzahl $n=p$ ist offensichtlich der Zähler $n!$ durch p teilbar, nicht aber der Nenner, da sowohl i als auch $n-i$ kleiner als $n=p$ sind. Somit ist $\binom{p}{i}$ für $1\le i\le p-1$ durch p teilbar, d.h. über einem Körper, der $\mathbb{F}_p$ enthält, ist $(a+b)^p = a^p+b^p$, und entsprechendes gilt auch für Summen mit mehr Summanden:

$$(a_1+\cdots+a_m)^p = a_1^p+\cdots+a_m^p\,.$$

Wenden wir dies speziell an für den Fall, daß alle Summanden gleich eins sind, so folgt $m^p = m\cdot 1^p = m$, d.h. jedes Element von $\mathbb{F}_p$ ist gleich seiner p-ten Potenz.

Falls wir nun ein Polynom $f\in\mathbb{F}_p[X]$ haben, dessen formale Ableitung identisch verschwindet, kommen in f nur Exponenten vor, die durch p teilbar sind; das Polynom hat also die Form

$$f = a_{dp}X^{dp} + a_{(d-1)p}X^{(d-q)p} + \cdots + a_pX^p + a_0\,.$$

Aus obiger Diskussion folgt, daß

$$\begin{aligned}&(a_{dp}X^d + a_{(d-1)p}X^{d-1} + \cdots + a_pX + a_0)^p\\ &= a_{dp}^pX^{dp} + a_{(d-1)p}^pX^{(d-1)p} + \cdots + a_p^pX^p + a_0^p\\ &= a_{dp}X^{dp} + a_{(d-1)p}X^{(d-1)p} + \cdots + a_pX^p + a_0 = f\end{aligned}$$

ist, Ein Polynom mit identisch verschwindender Ableitung über $\mathbb{F}_p$ ist somit die p-te Potenz eines anderen Polynoms. Beachtet man dies, läßt sich die quadratfreie Zerlegung leicht so modifizieren, daß sie auch über $\mathbb{F}_p$ funktioniert. Für uns ist das allerdings nicht weiter wichtig, da wir beim EZ GCD Algorithmus die quadratfreie Zerlegung bereits in $\mathbb{Q}[X]$ vornehmen.

Die Variante mit quadratfreier Zerlegung sieht folgendermaßen aus: Gegeben seien zwei primitive Polynome $f, g \in \mathbb{Z}[X]$. Führe in $\mathbb{Q}[X]$ die quadratfreie Zerlegung von f durch. Durch Multiplikation mit geeigneten rationalen Zahlen läßt sich erreichen, daß alle quadratfreien Faktoren g_j primitive Polynome aus $\mathbb{Z}[X]$ sind; f ist dann dargestellt als ein Produkt von Potenzen primitiver Polynome aus $\mathbb{Z}[X]$ mal einer rationalen Zahl. Da beide Seiten primitiv sind, kann diese nur plus oder minus eins sein.

Danach wende man den eingangs beschriebenen Algorithmus für jeden der quadratfreien Faktoren g_j an auf g_j und g. Falls nun nach der Reduktion modulo p der ggT h_j von g_j mod p und g mod p einen gemeinsamen Teiler mit g_j/h_j hat, ist g_j nicht mehr quadratfrei, und wir betrachten eine andere Primzahl.

Falls $\mathrm{ggT}(g_j, g)$ positiven Grad hat, müssen wir im Falle $j > 1$ noch den ggT von g_j und $g/\mathrm{ggT}(g, g_j)$ berechnen, um zu sehen, ob $\mathrm{ggT}(g_j^j, g)$ eventuell größer ist als $\mathrm{ggT}(g_j, g)$. Falls ja, muß das Verfahren iteriert werden, bis wir ggT eins bekommen. Das Produkt der so erhaltenen größten gemeinsamen Teiler ist dann der ggT von g_j^j und g, und der gesuchte ggT ist

$$\mathrm{ggT}(f, g) = \prod_{j=1}^{s} \mathrm{ggT}(g_j^j, g)\,.$$