Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Lösung polynomialer Gleichungen mit p-adischen Zahlen

Satz:
Sei $f \in \mathbb{Z}[X]$ und p eine Primzahl. Gibt es eine einfache Nullstelle von f in $\mathbb{Z}_p$, so gibt es auch eine einfache Nullstelle in in $\mathbb{Z}_{(p)}$.

Bemerkung: In Blatt 5 ging es um die Polynome $ax-1$ und x^k-a.
Der Beweis für beliebige Polynome ist aber nicht schwieriger.

Beweis:
Vorbemerkung:
Ein Polynom in $f=\mathbb{Z}[X]$ kann man als beiliebig oft differenzierbare reelle Funktion auffassen. Die Ableitung ist dann selbst ein Polynom in $\mathbb{Z}[X]$. Die Ableitung kann man aber auch als rein algebraisches Konstrukt auffassen. Für $f=\sum_{i=0}^{m} a_i x^i$ ist $f'=\sum_{i=0}^{m-1} (i+1)a_{i+1}x^i$: man braucht also keine Analysis, um die Abbildung $f \mapsto f'$ zu definieren. Diese ist eine Derivation, d.h. es gilt $(fg)'=f'g+fg'$, was sich auch rein algebraisch nachrechnen läßt. Es folgt sofort[1], daß f genau dann eine mehrfache Nullstelle in a besitzt, wenn wenn f'(a)=0. Entsprechendes gilt für Polynome in $\mathbb{Z}_p[X]$, $\mathbb{Z}_{p^\alpha}[X]$ und $\mathbb{Z}_{(p)}[X]$.

Im Satz wird das Polynom $f \in \mathbb{Z}[X]$ auch als Polynom in $\mathbb{Z}_p[X]$ interpretiert. Daß $a \in \mathbb{Z}_p$ eine einfache Nullstelle ist, heißt dann, daß $f'(a)$ als Element von $\mathbb{Z}_p$ ungleich Null ist oder daß $f'(a)$ in $\mathbb{Z}$ ausgewertet nicht durch p teilbar ist. Wir unterscheiden wieder nicht zwischen Elementen von $\mathbb{Z}_p$ und ihren Repräsentanten in $0,\ldots,p-1$.

Ersetzen wir in einem Polynom $f \in \mathbb{Z}[X]$ die Variable x durch x+h, so erhalten wir ein Polynom in den zwei Variablen x,h. Dieses Polynom in zwei Variablen können wir schreiben als Polynom in der Variablen h, mit Koffizienten in $\mathbb{Z}[X]$.

Ist z.B. $f=x^3+2x^2+3x+1$, so ist
$f(x+h)=x^3+3x^2h+3xh^2+h^3+2x^2+4xh+2h^2+3x+3h+1=$
$(x^3+2x^2+3x+1)+(3x^2+4x+3)h+(3x+2)h^2+h^3$
Die Polynome in x, die in dieser Formel als Koeffizienten der Potenzen von h auftauchen, erkennt man unschwer als $f, f' f''/2, f''/6$. Natürlich kommt das heraus auf die Taylorformel
$f(x+h)=\sum_{i=0}^{\operatorname{grad} f} (f^{(i)}(x)/i!)h^i$, welcher man aber nicht auf den ersten Blick ansieht, daß die Polynome, die als Koeffizienten der Potenzen von h auftauchen, keine gebrochenen Koeffizienten haben.

Jedenfalls läßt sich jetzt als Gleichung in $\mathbb{Z}[X]$ schreiben:
(*) $f(x+h)=f(x)+hf'(x)+h^2g(x)$, mit einem geeignete Polynom $g \in \mathbb{Z}[X]$.

Dabei braucht man gar nichts über Ableitungen zu wissen: $f'(x)$ ist einfach definitionsgemäß das Polynom, das sich als Koeffizient der ersten Potenz von h in obiger Umformung von $f(x+h)$ ergibt.

1 Zeigen Sie es!

Beginnen wir nun mit der Voraussetzung des Satzes:
Sei $f(x_0)=0$ in $\mathbb{Z}_p$ für $x_0\in\mathbb{Z}_p$ und $f'(x_0)\neq 0$ in $\mathbb{Z}_p$.

$f(x_0)=0$ in für $x_0\in\mathbb{Z}_p$ bedeutet: $f(x_0)=pk_0$ als Gleichung in $\mathbb{Z}$ mit einem geeigneten $k_0\in\mathbb{Z}$.

Rekursion:
Setzen wir $z_0:=x_0$.
Jetzt gehen wir davon aus, $x_0,\ldots,x_n$ seien bereits gefunden:
Es gelte also für $z_n:=\sum_{i=0}^{n} x_i p^i$, daß $f(z_n)=0\in\mathbb{Z}_{p^{n+1}}$.
Dann sollten wir also x_{n+1} so konstruieren, daß für $z_{n+1}:=z_n+x_{n+1}p^{n+1}$ gilt, daß $f(z_{n+1})=0$ in $\mathbb{Z}_{p^{n+2}}$. Gelingt diese rekursive Definition der Folge (x_n), so folgt sofort $f(\sum_{i=1}^{\infty} x_i p^i)=\lim_{n\to\infty} f(z_n)=0$
Damit ist auch eine p-adische Nullstelle von *f* gefunden.

$f(z_n)=0\in\mathbb{Z}_{p^n}$ bedeutet als Gleichung in $\mathbb{Z}$, daß $f(z_n)=p^{n+1}k_n$

$f(z_{n+1})=0$ in $\mathbb{Z}_{p^{n+2}}$ bedeutet in $\mathbb{Z}$, daß $f(z_{n+1})=p^{n+2}k_{n+1}$.
Andererseits folgt aus der fundamentalen Gleichung (*), daß
$f(z_{n+1})=f(z_n+x_{n+1}p^{n+1})=f(z_n)+f'(z_n)x_{n+1}p^{n+1}+(p^{n+1})^2(\text{ganze Zahl})=$
$p^{n+1}(k_n+f'(z_n)x_{n+1})+p^{n+2}(\text{ganze Zahl})$,

so daß ganz klar $k_n+f'(z_n)x_{n+1}$ durch *p* teilbar sein muß.
Um dies zu erreichen, müssen wir offenbar nur $x_{n+1}:=-k_n/f'(z_n)\in\mathbb{Z}_p$ berechnen!

Jetzt haben wir den Algorithmus:
Rekursionsanfang:
Finde $x_0=z_0\in\mathbb{Z}_p$ mit $f(z_0)=0\in\mathbb{Z}_p$ und $f'(z_0)\neq 0$. Setze $k_0:=f(z_0)/p$ in $\mathbb{Z}$.
Rekursionsschritt:
Setze $x_{n+1}:=-k_n/f'(z_n)\in\mathbb{Z}_p$, setze $z_{n+1}:=z_n+x_{n+1}p^{n+1}$ und $k_{n+1}:=f(z_{n+1})/p^{n+2}$

Beispiel:

1. Inversenbildung in $\mathbb{Z}_{(p)}$ einer ganzen Zahl a, die nicht durch p teilbar ist.
Das gemäß obiger Theorie zu betrachtende Polynom ist $f=a\,x-1$ und damit ist $f'=a$

```
invert(a,p,iter)={
   local(x=lift(1/Mod(a,p)),z=x,k=(a*z-1)/p,q=p);

   for(i=1,iter-1,
      x=lift(Mod(-k,p)/Mod(a,p));
      z=z+q*x;
      k=(a*z-1)/(q=q*p)
   );

   return(z)
}
```

Dabei ist iter die Anzahl der auszugebenden Stellen, p die Primzahl, a die zu invertierende Zahl.

Dazu noch als Hilfsfunktion

```
output(a,p)={
   local(v=a%p,w=a);
   while(w=w\p,v=concat(w%p,v));
   return(v)
}
```

welches eine natürliche Zahl zur Basis p darstellt, so daß man ggf. `output(invert(a,p,iter),p)` berechnen läßt; z,B. Berechnen wir hier 30 Stellen der p-adischen Entwicklung von 1/3 mit p=2:

```
(11:05) gp > output(invert(3,2,30),2)
%68 = [1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0,
1, 0, 1, 0, 1, 1]
```

2. Wurzelziehen

Zum Wurzelziehen berechnen wir eine Nullstelle des Polynoms $f = x^n - a$; dabei darf p kein Teiler von n sein (warum nicht?); demnach haben wir $f' = n x^{n-1}$.

```
root(a,n,p,iter)={
   local(
      x0=lift(Mod(a,p)^(1/n)),x=x0,z=x0,
      y0=1/Mod(n*x0^(n-1),p),
      k=(z^n-a)/p,
      q=p
   );

   for(i=1,iter-1,x=lift(Mod(-k,p)*y0);z=z+q*x;k=(z^n-a)/(q=q*p));
   return(z)
}
```

Dabei ist a die Zahl, aus der die n-te Wurzel gezogen werden soll, p die Primzahl, iter die Anzahl der Iterationen.

Tatsächlich kriege ich heraus:

(20:57) gp > root(123456789^17,17,5,12)
%37 = 123456789

11 Iterationen reichen nicht.

Bei einer größeren Primzahl p reichen weniger Iterationen
(20:59) gp > root(123456789^17,17,101,5)
%45 = 123456789