

Wurzelziehen modulo p^s

Sei p prim, $a \in \mathbb{N}$.

Ist $\left(\frac{a}{p}\right) = 1$, so ist die Gleichung $x^2 = a$ modulo p^s lösbar für alle $s \in \mathbb{N}$.

Es wird gezeigt: Ist $\left(\frac{a}{p}\right) = 1$, so ist die Gleichung $x^2 \equiv a$ modulo p^{s+1} lösbar, wenn sie modulo p^s lösbar ist. Daraus folgt offenbar durch Induktion die vorige Behauptung!

Sei $b^2 \equiv a \pmod{p^s}$. Dann gibt es also ein $c \in \mathbb{Z}$ mit $c p^s = b^2 - a$, d.h.

$b^2 - c p^s \equiv a \pmod{p^{s+1}}$. Macht man jetzt den Ansatz $(x p^s + b)^2 \equiv a \pmod{p^{s+1}}$, also $2 x b p^s + b^2 \equiv a \pmod{p^{s+1}}$, so ergibt sich zusammen mit $b^2 - c p^s \equiv a \pmod{p^{s+1}}$ $2 x b p^s + c p^s \equiv 0 \pmod{p^{s+1}}$, also $(2 x b + c) p^s \equiv 0 \pmod{p^{s+1}}$. Daraus folgt, daß $2 x b + c$ durch p teilbar sein muß. So ein x können wir aber leicht finden.

Umgekehrt folgt aus $2 x b + c \equiv 0 \pmod{p}$ auch $(x p^s + b)^2 \equiv a \pmod{p^{s+1}}$, d.h. wir haben eine Quadratwurzel aus a modulo p^{s+1} konstruiert.

Die obigen Überlegungen führen sofort zu folgendem Pari-Programm, welches die vorher definierte Funktion `root(a,p)` aufruft.

Dabei benutzen wir die Variable y statt wie oben im Text x , um das Polynom x , welches in `root` benutzt wird, nicht zu stören.

```
\\ root(a,p,s) berechnet die Wurzel aus a modulo p^s
root(a,p,s)=
{
    local(b,c,y);

    if(kronecker(a,p)!=1,
        print(a," besitzt keine Wurzel modulo ",p^s);
        return;
    );

    if(s==1,return(root(a,p)));

    b=root(a,p,s-1);c=((b^2-a)/p^(s-1));
    y=lift(Mod(-c,p)/Mod(2*b,p));
    return(y*p^(s-1)+b);
}
```

Hier nochmal die Funktion `root` mit der Korrektur von Dlugosch/Przigoda:

```
\\ Für jede Primzahl p>2 berechnet root(a,p) eine Quadratwurzel
\\ modulo p aus a, falls eine solche existiert.
```

```
root(a,p)=
{
```

```

local(i,b,f);
if(kronecker(a,p)!=1,
    print(a," besitzt keine Wurzel modulo ",p);
    return;
);

for(i=1,p-1,if(kronecker((b=i)^2-4*a,p)==-1,break;));

\\ b wird also so gewählt, daß  $b^2-a$  keine Wurzel mod  $p$  besitzt.

f=Pol(Mod(1,p)*x^2-Mod(b,p)*x+Mod(a,p));

\\ Damit ist das Polynom  $f$  in  $\mathbb{Z}_p[X]$  irreduzibel und daher
\\  $\mathbb{Z}_p[X]/\langle f \rangle$  ein Körper.

\\ In diesem Körper mit  $p^2$  Elementen, der  $\mathbb{Z}_p$  als
\\ Unterkörper enthält, liegt das Element  $x^{(p+1)/2}$ 
\\ in  $\mathbb{Z}_p$  und ist die gesuchte Wurzel! Also:

return(polcoeff(lift(lift(Mod(Mod(1,p)*x,f)^((p+1)/2))),0));
}

\\ Folgendes ergibt 403 als Wurzel von 27 modulo  $11^3$ :

root(27,11,3)

```