Quadrate und Wurzelziehen modulo *p*

Sei im Folgenden *p* eine Primzahl größer als 2.
Wir möchten im Körper $\mathbb{Z}_p$ Quadratwurzeln ziehen. Die Quadrierabbildung $Q:\mathbb{Z}_p^*\to\mathbb{Z}_p^* \quad x\mapsto x^2$ ist aber nicht surjektiv, daher gibt es Elemente von $\mathbb{Z}_p^*$, die keine Quadratwurzel besitzen.

Beispiel: *p*=17; In der zweiten Zeile stehen die Quadrate der Elemente in der ersten Zeile.
In der ersten Zeile stehen Quadratwurzeln der Elemente der zweiiten Zeile.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

Die Symmetrie in der zweiten Zeile rührt daher, daß mit $x^2=y$ natürlich auch $(-x)^2=y$ gilt; also haben in $\mathbb{Z}_{17}$ z.B. 10 und 7 dasselbe Quadrat, denn es ist 10=-7 . Man sieht, daß genau die Hälfte der Elemente von $\mathbb{Z}_{17}^*$ Quadrate sind. Ein Element von $\mathbb{Z}_{17}^*$ besitzt entweder keine oder genau zwei Quadratwurzeln. Man bemerkt auch, daß es i.a. einem Element nicht direkt anzusehen ist, ob es ein Quadrat ist und damit zwei Quadratwurzeln besitzt oder nicht. Das Element 0 in $\mathbb{Z}_p$ spielt eine Sonderrolle, da es das einzige Element von $\mathbb{Z}_p$ ist, welches nur eine Quadratwurzel besitzt; 0 gehört auch nicht zur multiplikativen Gruppe $\mathbb{Z}_p^*$.

Die Situation erhält mehr Struktur, wenn wir uns klarmachen, daß $Q:\mathbb{Z}_p^*\to\mathbb{Z}_p^*$ ein Gruppenhomomorphismus ist. Der Kern von *Q* besitzt genau zwei Elemente, nämlich 1 und -1=*p*-1. Dabei ist klar, daß $1,-1\in\ker Q$. Elemente des Kerns sind Nullstellen des Polynoms X^2-1 im Polynomring $\mathbb{Z}_p[X]$; wir wissen, daß ein Polynom zweiten Grades in diesem Ring höchstens zwei Nullstellen besitzen kann, daher gibt es keine weitere Elemente im Kern neben 1 und -1.

Die Bildmenge $Q(\mathbb{Z}_p^*)$, also die Menge der Quadrate, ist eine Untergruppe von $\mathbb{Z}_p^*$; sie besteht also aus den Elementen von $\mathbb{Z}_p^*$, die zwei Quadratwurzeln besitzen.

Aus der Gruppentheorie wissen wir, daß bei einem Gruppenhomomorphismus $\varphi:G\to H$ die Abbildung $\overline{\varphi}:G/\ker\varphi\to\varphi(G)$ ein Isomorphismus ist.Die Gruppen $\mathbb{Z}_p^*/\ker Q$ und $Q(\mathbb{Z}_p^*)$ sind also isomorph. Aus dem Satz von Lagrange folgt, daß $\mathbb{Z}_p^*/\ker Q$ genau halb so viele Elemente wie $\mathbb{Z}_p^*$ besitzt; dasselbe gilt somit für $Q(\mathbb{Z}_p^*)$, und wir wissen nun auch allgemein, daß $|Q(\mathbb{Z}_p^*)|=\frac{p-1}{2}$.

Da $|\mathbb{Z}_p^*|=p-1$, folgt aus dem Satz von Lagrange auch für jedes $x\in\mathbb{Z}_p^*$: $x^{p-1}=1$ [1].
Ist $y=x^2$, so ergibt sich daraus $1=x^{p-1}=(x^2)^{\frac{p-1}{2}}=y^{\frac{p-1}{2}}$. Dieselbe Folgerung läßt sich natürlich auch aus der Tatsache $|Q(\mathbb{Z}_p^*)|=\frac{p-1}{2}$ ziehen.

Ein beliebiges $x\in\mathbb{Z}_p^*$ genügt der Gleichung $\left(x^{\frac{p-1}{2}}\right)^2=x^{p-1}=1$, d.h. das Element $z:=\left(x^{\frac{p-1}{2}}\right)$ ist eine Nullstelle des Polynoms X^2-1 . Weil dieses Polynom nur zwei Nullstellen besitzen kann und 1 und -1 Nullstellen sind, kann *z* auch nur einen der beiden Werte 1 oder -1 annehmen. Oben wurde gezeigt, daß $x^{\frac{p-1}{2}}=1$, wenn *x* ein Quadrat ist. Es wäre jetzt natürlich schön, wenn für den Fall, daß

1 Diese Gleichung bezeichnet man auch als den „kleinen Satz von Fermat“.

x kein Quadrat ist, $x^{\frac{p-1}{2}}=-1$ gelten würde. Dann ließen sich nämlich Quadrate und Nicht-Quadrate durch den Wert von $x^{\frac{p-1}{2}}$ unterscheiden.

Nun könnte es ja sein, daß für alle Elemente von $x\in\mathbb{Z}_p^*$ die Gleichung $x^{\frac{p-1}{2}}=1$ gilt. Zwar ist die Gruppenordnung von $\mathbb{Z}_p^*$ gleich p-1, aber jedes einzelne Element könnte ja die Ordnung (p-1)/2 besitzen.

An dieser Stelle benutzen wir den **Satz**: $\mathbb{Z}_p^*$ ist zyklisch und verschieben den Beweis auf später.

Damit gibt es also einen Erzeuger $\xi\in\mathbb{Z}_p^*$ geben, der automatisch die Ordnung p-1 besitzt und für den deshalb die Gleichung $\xi^{\frac{p-1}{2}}=1$ nicht gelten kann. Ein $x\in\mathbb{Z}_p^*$ besitzt eine Darstellung $x=\xi^k$ und daher besitzt ein Quadrat $x^2\in\mathbb{Z}_p^*$ die Darstellung ξ^{2k} mit einem geraden Exponenten. Elemente in $\mathbb{Z}_p^*$ mit der Darstellung ξ^{2k+1} sind demnach keine Quadrate. Wir sehen jetzt sofort, daß das Produkt von einem Quadrat mit einem Nicht-Quadrat ein Nicht-Quadrat ist und das Produkt von zwei Nicht-Quadraten ein Quadrat ist. Weil ξ die Ordnung p-1 besitzt und daher nicht $\xi^{\frac{p-1}{2}}=1$ gilt, ist demnach $\xi^{\frac{p-1}{2}}=-1$. Für ein Nicht-Quadrat $x\in\mathbb{Z}_p^*$ folgt dann $x^{\frac{p-1}{2}}=\left(\xi^{2k+1}\right)^{\frac{p-1}{2}}=\left(\xi^{\frac{p-1}{2}}\right)^{2k+1}=(-1)^{2k+1}=-1$, und genau dieses Ergebnis haben wir oben angestrebt.

Zusammenfassung:
Quadrate in $\mathbb{Z}_p^*$ sind charakterisiert durch die Gleichung $x^{\frac{p-1}{2}}=1$,
Nicht-Quadrate sind charakterisiert durch die Gleichung $x^{\frac{p-1}{2}}=-1$

Schauen wir uns noch einmal das Beispiel p=17 an. ξ=3 ist Erzeuger von $\mathbb{Z}_{17}^*$:

ξ^0	ξ^1	ξ^2	ξ^3	ξ^4	ξ^5	ξ^6	ξ^7	ξ^8	ξ^9	ξ^{10}	ξ^{11}	ξ^{12}	ξ^{13}	ξ^{14}	ξ^{15}
1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

In der zweiten Zeile sind die Potenzen der ersten Zeile konkret ausgerechnet. Wir sehen, wie die Einträge mit geradem Exponenten genau die Quadrate aus der vorigen Tabelle sind. Die ungeraden Potenzen sind dann gerade die übrigen Elemente von $\mathbb{Z}_{17}^*$, also die Nicht-Quadrate. Es sollte auch auffallen, daß die Potenzen von ξ=3 recht wild in $\mathbb{Z}_{17}^*$ herumspringen!

Die obigen Überlegungen zeigen auch, daß die Abbildung $\Phi:\mathbb{Z}_p^*\to\{1,-1\}$, $x\mapsto x^{\frac{p-1}{2}}$ ein Gruppenhomomorphismus ist, dessen Kern gerade die Gruppe der Quadrate ist, also $Q(\mathbb{Z}_p^*)$. Dazu sei noch bemerkt, daß sowohl $\Phi\circ Q$ wie auch $Q\circ\Phi$ alle Elemente von $\mathbb{Z}_p^*$ auf die 1 abbilden.

Nach diesen Vorbereitungen kommen wir zum **Wurzelziehen**:

Methode 1:
Sei p eine Primzahl größer als 2 mit $p \equiv 3 \bmod 4$[2]. Die Hälfte der Primzahlen erfüllt diese Bedingung.

Wir wissen daß ein Element $x \in \mathbb{Z}_p^*$ genau dann ein Quadrat ist, wenn $x^{\frac{p-1}{2}} = 1$ gilt.
Ist diese Voraussetzung erfüllt, so ist $w := x^{\frac{p+1}{4}}$ eine Quadratwurzel von x, also $w^2 = x$.
Damit ist natürlich $-w$ die zweite Quadratwurzel von x.

Beweis: Es ist $w^2 = \left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}+1} = x^{\frac{p-1}{2}} \cdot x = 1 \cdot x = x$.

Bemerkung: Man kann sich die Überprüfung der Voraussetzung $x^{\frac{p-1}{2}} = 1$ auch sparen:
Es ist ja jedenfalls $w^2 = \left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}+1} = x^{\frac{p-1}{2}} \cdot x = \pm 1 \cdot x = \pm x$. Wenn also $w^2 = x$, dann haben wir eine Quadratwurzel von x berechnet; wenn $w^2 = -x$, dann besitzt x keine Wurzel.

Beispiel

Für p=19 betrachten wir x=5. In $\mathbb{Z}_{19}^*$ gilt $5^{\frac{19-1}{2}} = 5^9 = 1$, also ist 5 ein Quadrat in $\mathbb{Z}_{19}^*$.
Weil $19 \equiv 3 \bmod 4$, können wir die obige Formel anwenden und haben mit $9 = 5^{\frac{19+1}{4}}$ eine Wurzel gefunden: tatsächlich ist $9^2 = 5$ in $\mathbb{Z}_{19}^*$.

Methode 2:
Die jetzt folgende Methode zum Wurzelziehen funktioniert in $\mathbb{Z}_p^*$ für alle ungeraden Primzahlen p.
Zu ihrer Herleitung kommt unser gesamtes Arsenal zum Einsatz.
Wir gehen aus von einem Quadrat $a \in \mathbb{Z}_p^*$; wir wissen also, daß $a^{\frac{p-1}{2}} = 1$.

Es wird nun ein Polynom $f = X^2 + bX + a \in \mathbb{Z}_p[X]$ gesucht, welches irreduzibel ist. Dabei sei der Koeffizient a das Element, aus dem die Wurzel gezogen werden soll, während b so gewählt werden muß, daß f tatsächlich irreduzibel wird. Wäre f nicht irreduzibel, so zerfiele es in Polynome ersten Grades, man hätte also $f = (X+u)(X+v) = X^2 + (u+v)X + uv$, demnach $b=u+v$, $a=uv$, also $b^2 = u^2 + 2uv + v^2$, also $b^2 - 4a = u^2 + 2uv + v^2 - 4uv = u^2 - 2uv + v^2 = (u-v)^2$. Damit wäre $b^2 - 4a$ ein Quadrat in $\mathbb{Z}_p^*$, also $(b^2-4a)^{\frac{p-1}{2}} = 1$. Probieren wir also die $b \in \mathbb{Z}_p$ durch, bis $(b^2-4a)^{\frac{p-1}{2}} = -1$, so haben wir anschließend automatisch ein irreduzibles Polynom.

Daß wir b immer so finden können daß $b^2 - 4a$ kein Quadrat ist, begründen wir wie folgt:
Ist $p \equiv 3 \bmod 4$ wie oben, so ist $(-1)^{\frac{p-1}{2}} = -1$, also -1 kein Quadrat in $\mathbb{Z}_p^*$. Setzen wir b=0, so ist $b^2 - 4a = (-1)\cdot(4a)$ das Produkt von einem Nicht-Quadrat mit einem Quadrat, also kein Quadrat.

Ist dagegen $p \equiv 1 \bmod 4$, so ist $(-1)^{\frac{p-1}{2}} = 1$, also -1 ein Quadrat in $\mathbb{Z}_p^*$ und damit ist $-4a$=(-1)4(a) als

2 Sind $a, b, c \in \mathbb{Z}$, so soll die Schreibweise $a \equiv b \bmod c$ bedeuten, daß $a - b \in c\mathbb{Z}$, daß also $a \,\%\, c = b \,\%\, c$.

Produkt von Quadraten ein Quadrat, sagen wir $-4a = c^2$.

Wir wissen, daß nicht alle Elemente von $\mathbb{Z}_p^*$ Quadrate sind. Sei *k* das kleinste Element in der Folge $1, \ldots, p-1$, welches kein Quadrat ist. Dann ist *k*-1 Quadrat, sagen wir $k-1 = d^2$ und $k = d^2+1$ ist kein Quadrat. Setzen wir jetzt *b*=*cd*, so wissen wir, daß $b^2-4a = b^2+c^2 = c^2((b/c)^2+1) = c^2(d^2+1)$. Am Schluß steht ein Produkt von einem Quadrat und einem Nicht-Quadrat, also ein Nicht-Quadrat und b^2-4a ist tatsächlich ein Nicht-Quadrat.

Haben wir nun das Ziel erreicht, daß das Polynom $f = X^2+bX+a \in \mathbb{Z}_p[X]$ irreduzibel ist, so können wir im Körper $K := \mathbb{Z}_p[X]/<f>$ rechnen, welcher p^2 Elemente besitzt. Wir können $\mathbb{Z}_p$ als Unterkörper von *K* auffassen, indem wir ein Element $a \in \mathbb{Z}_p$ mit der Restklasse $\overline{a}$ eines Polynoms 0-ten Grades identifizieren bzw. mit der Restklasse des Nullpolynoms, wenn *a*=0.

Die Elemente von *K* sind Restklassen modulo *f* von Polynomen höchstens 1. Grades. Eine dieser Restklassen ist $\overline{X}$, und man hat sofort, daß $f(\overline{X}) = \overline{f(X)} = \overline{0}$. Unser Polynom, welches in $\mathbb{Z}_p$ keine Nullstelle besaß, hat also jetzt eine in *K*!

In $\mathbb{Z}_p$, $\mathbb{Z}_p[X]$ und *K* nimmt die binomische Formel mit Exponent *p* die einfache Form $(x+y)^p = x^p+y^p$, oder auch $(x+y+z)^p = x^p+y^p+z^p$ an, denn die Binomialkoeffizienten in den gemischten Termen sind alle durch *p* teilbar und fallen daher beim Rechnen in $\mathbb{Z}_p$ weg. Und für ein Element $x \in \mathbb{Z}_p$ gilt bekanntlich $x^{p-1} = 1$, also $x^p = x$.

Daher ergibt sich $\overline{0} = f(\overline{X})^p = (\overline{X}^p)^2 + b^p\overline{X}^p + a^p = (\overline{X}^p)^2 + b\overline{X}^p + a$, und wir haben mit $\overline{X}^p$ eine zweite Nullstelle von *f* in *K*[*X*] gefunden. Es ist auch $\overline{X}^p \neq \overline{X}$. Der Grund dafür liegt darin daß sonst $\overline{X}^p - \overline{X} = \overline{0}$ wäre und somit $\overline{X}$ eine Nullstelle des Polynoms $X^p - X$. Dieses Polynom besitzt aber bereits alle Elemente von $\mathbb{Z}_p$ als Nullstellen. Als Polynom *p*-ten Grades kann es nicht mehr als *p* Nullstellen besitzen, und $\overline{X}$ wäre eine weitere.

In *K*[*X*] gilt demnach: $f = (X-\overline{X})(X-\overline{X}^p) = X^2+bX+a$, also ist $\overline{X}^{p+1} = \overline{X}\cdot\overline{X}^p = a$.

Es gilt daher $\left(\overline{X}^{\frac{p+1}{2}}\right)^2 = a,$ und damit haben wir eine Quadratwurzel von *a*! Es wäre unangenehm, wenn diese Wurzel in $K \setminus \mathbb{Z}_p$ läge. Wir wissen aber bereits, daß *a* in $\mathbb{Z}_p$ zwei Quadratwurzeln besitzt; diese Quadratwurzeln sind Nullstellen des quadratischen Polynoms X^2-a , und dieses Polynom kann auch in *K* nicht mehr als zwei Nullstellen besitzen! Daher liegt das Element $\overline{X}^{\frac{p+1}{2}}$ bereits in $\mathbb{Z}_p \subset K$, und ist eine der beiden gesuchten Quadratwurzeln von *a*!

Hier also noch einmal der **Algorithmus**:

Gegeben sei eine ungerade Primzahl *p* und ein Element $a \neq 0 \in \mathbb{Z}_p$, welches eine Quadratwurzel besitzt, für welches also $a^{\frac{p-1}{2}} = 1$ in $\mathbb{Z}_p$ gilt.

Man suche ein $b \in \mathbb{Z}_p$, so daß $(b^2-4a)^{\frac{p-1}{2}} = -1$, bilde das Polynom $f = X^2+bX+a \in \mathbb{Z}_p[X]$.

Wir berechnen das Element $\overline{X}^{\frac{p+1}{2}}$ in $K := Z_p[X]/<f>$.
Dieses liegt bereits in $\mathbb{Z}_p$ und ist eine der Quadratwurzeln von *a*.

Beispiel:

Wir prüfen, ob a=2 eine Quadratwurzel in $\mathbb{Z}_{17}$ besitzt. Dazu schauen wir nach, ob $2^{\frac{17-1}{2}}=1$, was tatsächlich der Fall ist. Anschließend bestimmen wir b so, daß b^2-4a kein Quadrat in $\mathbb{Z}_{17}$ ist, indem wir sukzessive für b=0,1,... überprüfen, ob $(b^2-4a)^{\frac{p-1}{2}}=-1$ wird. Dies ist schon für b=1 der Fall.

Es ist also $f=X^2+X+2$ irreduzibel in $\mathbb{Z}_{17}[X]$.

Berechnen wir jetzt manuell: $(\overline{X})^{\frac{17+1}{2}}$ in $K:=\mathbb{Z}_{17}[X]/<f>$, lassen aber zur Schreiberleichterung die Äquivalenzklassenstriche weg:

$X^9=(((X^2)^2)^2)X$

$X^2=X^2-f=-X-2, X^4=(-X-2)^2=X^2+4X+4=X^2+4X+4-f=3X+2$

$X^8=(3X+2)^2=9X^2+12X+4=9X^2+12X+4-9f=3X-14=3X+3$

$X^9=3X^2+3X=3X^2+3X-3f=-6=11$

Wie erhofft, kommt in diesem letzten Ergebnis kein X mehr vor, und wir sehen sofort die Quadratwurzeln 11 und 6 von 2 in $\mathbb{Z}_{17}$.