Modulare Quadratwurzeln beim Fiat-Shamir-Verfahren zur Authentikation

(zu „Grundkurs Codierung“, 3. Auflage 2006, Vieweg Verlag, ISBN 3-528-25399-1,
Unterkapitel 5.10, Seiten 303 ff)
update vom 20.03.1996

Bei der Darstellung des Fiat-Shamir-Authentikations-Verfahrens waren folgende zwei Fragen ohne Antwort geblieben:

1. Warum soll die (geheime) Schlüsselzahl s und die Testzahl r teilerfremd zum Modul n = p·q sein?
2. Warum ist die Bestimmung der modularen Quadratwurzel s in der Beziehung $v = s^2$ MOD n, oder genauer der beiden Wurzeln ± s, dann in praktikabler Zeit undurchführbar, wenn man die beiden Primzahlen p und q nicht kennt, aus denen sich der Modul n = p·q zusammensetzt?

Zu Frage 1: Teilerfremde Zahlen s und r zum Modul n

Wenn eine oder beide Zahlen s und r gemeinsame Teiler mit dem Modul n = p·q haben, so lassen sich die Faktoren p oder q direkt ermitteln. Wie aus der Antwort auf Frage 2 hervorgeht, ist damit die Sicherheit des gesamten Verfahrens ausgehebelt.

Der Grund liegt in der Eigenschaft der Modulo-Funktion, dass gemeinsame Teiler im Ergebnis erhalten bleiben. Schon bei der Untersuchung des RSA-Algorithmus wurde festgestellt, dass eine zu n *nicht* teilerfremde Zahl r < p·q nur einen der beiden Faktoren p oder q enthalten kann, dies je nach den Größenverhältnissen zwischen p und q aber auch als Potenz. Nimmt man dafür z. B. p, so stellt sich dies allgemein als

$$r = t \cdot p^a , \qquad t, a \text{ natürliche Zahlen} \geq 1$$

dar. Da die Modulo-Funktion den Rest der Division durch den Modul n ermittelt, lässt sich ein gemeinsamer Faktor (= gemeinsamer Teiler) vor das Ergebnis ziehen. Aus der Definition der Modulo-Funktion

$$r = t \cdot p^a = i \cdot (p \cdot q) + \text{Rest} , \qquad \text{mit } 0 \leq \text{Rest} < (p \cdot q)$$

folgt andererseits

$$\text{Rest} = t \cdot p^a - i \cdot (p \cdot q) = p \cdot (t \cdot p^{a-1} - i \cdot q).$$

Der Rest enthält also einen Faktor p. Bildet man mit dem Euklidischen Algorithmus den ggT(Rest,n), dann liefert er gerade diesen Faktor und über q = n/p ist auch der zweite bekannt.

Dies gilt in gleicher Weise nicht nur für r, sondern ebenfalls für s und für jede andere natürliche Zahl, z. B. r·s. Wesentlich ist dabei, dass man weder r noch s noch r·s selbst kennen muss, sondern nur den Modulo (p·q)-Wert dieser Zahlen. Im folgenden Beispiel wird angenommen, dass die Zerlegung des Moduls n in die beiden Primfaktoren p·q unbekannt ist. Der eine Partner im Authentikationsverfahren habe ohne weitere Prüfung die Zufallszahl r gewählt. Damit liegen vor:

$$n = 377 \qquad r = 91$$

Er quadriert r und bildet mit MOD n das Ergebnis

$$r^2 \text{ MOD } n = 8281 \text{ MOD } 377 = 364.$$

Diese Zahl schickt er seinem Partner. Wenn dieser mit dem Euklidischen Algorithmus den ggT(364, 377) berechnet, erhält er

$$377 = 1\ 364 + 13$$
$$364 = 28\ 13 + 0.$$

Er weiß dann ohne großen Aufwand, dass 13 der größte gemeinsame Teiler von 364 und 377 ist und, *viel schlimmer*, dass 13 den einen Faktor von n darstellt. Damit steht ihm auch n/13 = 29 zur Verfügung und die Sicherheit des gesamten Verfahrens ist - in diesem Fall – zerstört.

Zu Frage 2: Bestimmung der modularen Quadratwurzeln

Zerlegung in zwei Teilaufgaben

Wählt man als Modul statt einer aus den beiden Primzahlen p·q zusammengesetzten Zahl n nur eine Primzahl p, so lassen sich die beiden Quadratwurzeln ± s unmittelbar aus dem modularen Quadrat

$$v_p = s^2 \text{ MOD } p$$

berechnen. Wir werden uns den dafür geeigneten Algorithmus sogleich ansehen (*erste Teilaufgabe*). Aber auch dann, wenn der Modul aus dem Produkt zweier bekannter Primzahlen p und q (oder aus weiteren bekannten Primzahlen) besteht, ist die Berechnung der modularen Quadratwurzel schnell zu erledigen (*zweite Teilaufgabe*).

Erste Teilaufgabe: *Algorithmus zur Bestimmung der modularen Quadratwurzeln in einem endlichen Zahlenkörper* Z_p

Sehen wir uns zunächst also den Algorithmus zur Berechnung der modularen Wurzel an, wenn der Modul eine Primzahl p ist. Modulare Quadratzahlen v_p werden in der Literatur auch als quadratische Reste bezeichnet. Nimmt man den trivialen Fall der Null einmal aus, so gibt es in endlichen Körpern Z_p immer genau (p-1)/2 quadratische Reste, die andere Hälfte sind nichtquadratische Reste w_p. Zu letzteren existieren natürlich auch keine Quadratwurzeln innerhalb der p verschiedenen Elemente 0,1,2,3, ... , p-2, p-1 dieses Körpers.

Tabelle 1 zeigt ein Beispiel mit p = 13. Wie man sieht, gibt es zu 2, 5, 6, 7, 8 und 11 keine Quadratwurzel, wohl aber zu 1, 3, 4, 9, 10 und 12. Mithilfe der *Legendre-Funktion* (x/p), auch Legendre-Symbol genannt (es ist **nicht** der Quotient x/p !), kann man leicht prüfen, ob eine vorgegebene Zahl x einen quadratischen oder einen nichtquadratischen Rest bezüglich p darstellt, siehe z. B. *dtv-Atlas zur Mathematik, 7.Auflage 1987, S. 121*.

Elements	modulares Quadrat $v_p = s^2$ MOD 13	Wurzeln ±s	
0	0	±0	
1	1	1	-1 = 12
2	4	2	-2 = 11
3	9	3	-3 = 10
4	3	4	-4 = 9
5	12	5	-5 = 8
6	10	6	-6 = 7
7	10	7	-7 = 6
8	12	8	-8 = 5
9	3	9	-9 = 4
10	9	10	-10 = 3
11	4	11	-11 = 2
12	1	12	-10 = 1

Tabelle 1: Modulare Quadrate (= quadratische reste) im endlichen Körper Z_{13}

Falls der Wert des Ausdrucks

$$(x/p) = x^{(p-1)/2} \text{ MOD } p = 1$$

beträgt, ist x ein modulares Quadrat, also ein quadratischer Rest v_p, falls man

$$(x/p) = x^{(p-1)/2} \text{ MOD } p = -1 \qquad = p-1$$

erhält, handelt es sich bei x um einen nichtquadratischen Rest w_p. Da, wie bereits erwähnt, quadratische und nichtquadratische Reste in jedem Zahlenkörper in gleicher Anzahl vorhanden sind, kommt man beim Austesten willkürlich gewählter Zahlen bereits nach wenigen Versuchen auf Beispiele aus beiden Gattungen. Im Z_{13} etwa ergibt sich für x = 7 der Wert

$$(7/13) = 7^{(12/2)} \text{ MOD } 13 = 7^{6} \text{ MOD } 13 \qquad = 117\,649 \text{ MOD } 13 = 12 \qquad = -1.$$

7 ist also ein nichtquadratischer Rest bezüglich 13, was auch die Tabelle 1 zeigt.

Der Wert x = 10 hingegen erweist sich wegen

$$(10/13) = 10^{6} \text{ MOD } 13 = 1\,000\,000 \text{ MOD } 13 \qquad = 1$$

als quadratischer Rest. Allerdings muss man sich mit dieser Kenntnis zunächst begnügen, da die Legendre-Formel keine Möglichkeit zur Berechnung der beiden zugehörigen modularen Wurzeln ±s selbst bietet. Dies ermöglicht der bei *Neal Koblitz in „A Course in Number Theory and Cryptography", Springer-Verlag, 1987, §2, S. 47 ff*, beschriebene Algorithmus, für dessen Anwendung das Legendre-Theorem nützlich ist. Wir verwenden einen leicht veränderten Weg.

Die Idee lässt sich erläutern, wenn man die Darstellung der p-1 Körperelemente s als Potenzen eines primitiven Elementes z dieses Körpers verwendet. Ein solches primitives Element hat die Eigenschaft, dass hieraus durch Potenzieren jedes Element s genau einmal gebildet werden kann. Die folgende Tabelle zeigt dies für p = 13 und z = 2:

Potenz z^i MOD 13 = s des primitiven Elements z = 2		
2^1 MOD 13	= 2 MOD 13	= 2
2^2 MOD 13	= 4 MOD 13	= 4
2^3 MOD 13	= 8 MOD 13	= 8
2^4 MOD 13	= 16 MOD 13	= 3
2^5 MOD 13	= 32 MOD 13	= 6
2^6 MOD 13	= 64 MOD 13	= 12
2^7 MOD 13	= 128 MOD 13	= 11
2^8 MOD 13	= 256 MOD 13	= 9
2^9 MOD 13	= 512 MOD 13	= 5
2^{10} MOD 13	= 1024 MOD 13	= 10
2^{11} MOD 13	= 2048 MOD 13	= 7
2^{12} MOD 13 = 2^0 MOD 13	= 4048 MOD 13 = 1 MOD 13	= 1

Tabelle 2: Elemente s des Körpers Z_{13} als Potenzen des primitiven Elements z = 2

Endliche Zahlenkörper haben im allgemeinen mehrere solcher primitiven Elemente, die aber gleichwertig sind, so dass die Wahl von z = 2 keine Besonderheit darstellt. Natürlich können nur solche Elemente s modulare Quadrate v_p sein, deren Potenz von z eine gerade Zahl darstellt, da beim „Wurzelziehen" der Exponent halbiert wird und dabei wieder ein ganzahliges Element (des Körpers) herauskommen muss. So ist z.B. $s = 3 = 2^4$ MOD 13 ein modulares Quadrat und die zugehörigen Wurzeln sind $\pm 2^2$ MOD 13 = ± 4, mit -4 MOD 13 = 9. Ein Vergleich der Tabellen 1 und 2 zeigt die Übereinstimmung. Außerdem wird hieran deutlich, dass z. B. 2^{11} MOD 13 = 7 kein quadratischer Rest sein kann.

Die Potenzen sind im übrigen bei endlichen Zahlenkörpern nur bis auf eine Faktor p-1 eindeutig, bei höheren Potenzen wiederholt sich alles im Abstand von jeweils p-1, der so genannten *Ordnung* von Z_p. Auf die Exponenten ist also immer die Modulo-Bildung mit MOD p-1 anzuwenden. Man erkennt das z. B. in der letzten Tabellenzeile an 2^{12} MOD 13 = 2^0 MOD 13 = $2^{\,12 \text{ MOD } 12}$ MOD 13 = 1. Genauso gilt 2^{14} MOD 13 = $2^{\,14 \text{ MOD } 12}$ 2^2 MOD 13 = 4 usw.

Wir nehmen nun an, dass ein quadratischer Rest v_p , z. B. v_p =10, vorliegt, was mit der Legendre-Formel überprüft wurde. Wenn die Potenzdarstellung $10 = 2^{10}$ MOD13 bekannt wäre, müsste man durch irgendeine Veränderung erreichen, dass dabei eine Potenz MOD 12 mit dem halben Exponenten heraus käme, also 2^5 , womit die gesuchten Wurzeln $\pm 2^5$MOD 13 = ±6 bekannt wären. Wie lässt sich das erreichen?

Man kann v_p mit einer Potenz des primitiven Elementes 2 multiplizieren, wobei hierfür ein geeigneter Exponent i gewählt wurde. Bei dieser Multiplikation werden die Exponenten beider Multiplikanden addiert. Da der Ex-

ponent des Ergebnisses selbst wieder gerade oder ungerade sein kann, nimmt man zweckmäßigerweise eine ungerade Potenz und passt diese durch systematisches Potenzieren nochmals an. Eine solche ungerade Potenz haben aber alle nichtquadratischen Reste w_p. Durch Austesten wurde dafür etwa $11 = 2^7$ MOD 13 gefunden. Für das Beispiel mit $v_p = 10 = 2^{10}$ MOD 13 heißt dies:

$$v_p \cdot 2^i = 2^{10} \cdot 2^7 \text{ MOD } 13 = 2^{17} \text{ MOD } 13 = 2^{17 \text{ MOD } 12} \text{ MOD } 13 = 2^5 \text{ MOD } 13 = 6$$

Damit wäre das richtige Ergebnis bereits erreicht. Mit einem anderen nichtquadratischen Rest $w_p = 2^9$ MOD 13 = 5 hätte es allerdings nicht auf Anhieb funktioniert, da

$$v_p \cdot 2^i = 2^{10} \cdot 2^9 \text{ MOD } 13 = 2^{19} \text{ MOD } 13 = 2^{19 \text{ MOD } 12} \text{ MOD } 13 = 2^7 \text{ MOD } 13 = 11$$

ist und auch Potenzen $(2^9)^2$ oder $(2^9)^3$ oder $(2^9)^4$ nicht weiterführen, wie man an den resultierenden Exponenten erkennt. In dieser Form ist das Verfahren also noch nicht brauchbar, da man natürlich einen sicheren Weg benötigt. Aber die grobe Richtung des Vorgehens stimmt bereits.

Um zum richtigen Ergebnis zu gelangen, wendet man eine Verfeinerung an. Dazu zerlegt man die Eulerzahl $\varphi(p) = p-1$ in einen Faktor der größtmöglichen Zweierpotenzen 2^α und in eine ungerade Zahl b

$$\varphi(p) = p-1 = 2^\alpha \cdot b$$

und berechnet

$$c = v_p^{(b+1)/2} \text{ MOD } p.$$

Bei p=13 ist $\varphi(p) = p-1 = 12 = 2^2 \cdot 3$, also $\alpha = 2$, $b = 3$.

Für den quadratischen Rest $v_p = 2^{10}$ MOD 13 = 10 bedeutet dies

$$c = (2^{10})^{(3+1)/2} \text{ MOD } 13 = 2^{20 \text{ MOD } 12} \text{ MOD } 13 = 2^8 \text{ MOD } 13.$$

Außerdem berechnet man mit irgendeinem nichtquadratischen Rest w_p dessen b-te Potenz

$$d = w_p^b \text{ MOD } p.$$

Mit $w_p = 2^9$ MOD 13 ergibt sich also

$$d = (2^9)^3 \text{ MOD } 13 = 2^{27 \text{ MOD } 12} \text{ MOD } 13 = 2^3 \text{ MOD } 13 = 8.$$

Nun bildet man das modulare Produkt

$$c \cdot d = 2^8 \cdot 2^3 \text{ MOD } 13 = 2^{11} \text{ MOD } 13 = 7.$$

Die Probe 7^2 MOD 13 = 10 zeigt, dass das Ergebnis noch nicht vorliegt. Deshalb versuchen wir systematisch die nächste Potenz von d:

$$c \cdot d^2 = 2^8 \cdot 2^6 \text{ MOD } 13 = 2^{14 \text{ MOD } 12} \text{ MOD } 13 = 2^2 \text{ MOD } 13 = 4.$$

Auch das ist nicht richtig, aber mit

$$c \cdot d^3 = 2^8 \cdot 2^9 \text{ MOD } 13 = 2^{17 \text{ MOD } 12} \text{ MOD } 13 = 2^5 \text{ MOD } 13 = 6.$$

sind wir erfolgreich. Die Probe ergibt nämlich, dass wir jetzt das gewünschte Ergebnis erhalten haben (man muss nur noch zusätzlich die negative Wurzel -6 MOD 13 = 7 berechnen, damit es vollständig wird).

Der soeben skizzierte Weg führt immer zum Ziel - im ungünstigsten Fall nach höchstens (α-1)-Versuchen, was wir uns jetzt klar machen werden. Allgemein gilt:

$$v_p = z^{2k} \qquad \text{mit } 0 \le k \le (p-1)/2,$$

sowie

$$w_p = z^m \qquad \text{mit } 1 \le m \le (p-1).$$

Für c und d ergibt sich deshalb

$$c = z^{2k\cdot(b+1)/2} = z^{k\cdot(b+1)}$$

$$d^i = z^{mi\cdot b} \qquad \text{mit } 0 \le i \le 2^{\alpha-1}\ .$$

Das Produkt wird

$$c\cdot d^i = z^{k\cdot(b+1) + i\cdot m\cdot b}$$

Die Frage ist nun, ob bei geeigneter Wahl von i immer der Exponent k herauskommt:

$$c\cdot d^i = z^{k\cdot(b+1) + i\cdot m\cdot b} = z^{k\cdot(b+1) + i\cdot m\cdot b \ \text{MOD}\ p-1} = z^{k\cdot(b+1) + i\cdot m\cdot b \ \text{MOD}\ 2\alpha b} = z^k \ ?$$

Da z als Basis auf beiden Seiten steht, genügt es, nur den Exponenten zu betrachten:

$$(k\cdot(b+1) + i\cdot m\cdot b) \ \text{MOD}\ 2^\alpha b = k\ ?$$

Nach Vereinfachung und wegen $b \neq 0$ gilt auch

$$(k + i\cdot m) \ \text{MOD}\ 2^\alpha = 0\ ?$$

Man kann also fragen, ob man zu jedem vorgegebenen k, m und α ein i findet, dass diese Gleichung erfüllt. Die Antwort ist „ja“. Warum?

Da m eine ungerade Zahl darstellt, ist sie mit 2^∞ teilerfremd. Insbesondere gilt

$$m \ \text{MOD}\ 2^\alpha \neq 0.$$

Ein Produkt $(i\cdot m)$ MOD 2^α kann wegen der Teilerfremdheit $ggT(m, 2^\alpha) = 1$ nur dann Null werden, wenn i ein Vielfaches von 2^α darstellt. Für alle anderen Werte i = 1, 2, 3, ..., $2^{\alpha-1}$ -1 MOD 2^α nimmt auch das Produkt $(i\cdot m)$ MOD 2^α genau einmal jeden Wert 1, 2, 3, ..., $2^{\alpha-1}$-1 MOD 2^α an. Tabelle 3 gibt für m = 3, m = 7, $2^\alpha = 4$ und $2^\alpha = 8$ je ein Beispiel.

Für den allgemeinen Fall kann man sich dies folgendermaßen klarmachen: Für i=1 und $m < 2^\alpha$ ist

$$m \ \text{MOD}\ 2^\alpha = m.$$

Für $2\,m \ \text{MOD}\ 2^\alpha = m'$

kann das Ergebnis m’ nicht 0 sein, wenn $2 \neq 2^\alpha$ ist. Es kann aber auch nicht m’ = m sein, weil sich dann das Ergebnis auch im nächsten Schritt für $3\cdot m$ MOD 2^α nicht ändern würde und so für $i\cdot m = 2^\alpha\cdot m$ nie 0 entstehen könnte. Also ist $m' \neq m$. Das Ergebnis des dritten Schritts

$$3\,m \ \text{MOD}\ 2^\alpha = m''$$

ist wieder von m' verschieden, also m'' ≠ m', es kann aber auch nicht m sein, da 4·m MOD 2^{α} dann m' wäre und bei i·m= i ·2^{α} MOD 2^{α} wiederum keine 0 erscheinen könnte. Damit ist klar, dass es immer einen Wert i gibt, der den Wert von k mit dem modularen Produkt i·m MOD 2^{α} auf ein Vielfaches von 2^{α} ergänzt. Für m > 2^{α} gilt dasselbe, da sich m dann aus m = t·2^{α} + m* zusammensetzt, wobei t = 1, 2, 3, 4, ... und 1 ≤ m* ≤ 2 $^{\alpha}$-1 ist.

i	i·3	i·3 MOD 4	i·3 MOD 8	i·7	i·7 MOD 4	i·7 MOD8
1	3	3	3	7	3	7
2	6	2	6	14	2	6
3	9	1	1	21	1	5
4	12	0	4	28	0	4
5	15	3	7	35	3	3
6	18	2	2	42	2	2
7	21	1	5	49	1	1
8	24	0	0	56	0	0
9	27	3	3	63	3	7
10	30	2	6	70	2	6
11	33	1	1	77	1	5
12	36	0	4	84	0	4
13	39	3	7	91	3	3
14	42	2	2	98	2	2
15	45	1	5	105	1	1
16	48	0	0	112	0	0
17	51	3	3	119	3	7

Tabelle 3: Modulare Produkte i·m

Der Lösungsweg wird nun noch einmal zusammen gefasst, wobei erneut zu betonen ist, dass hierbei an keiner Stelle eine Notwendigkeit zur Kenntnis eines primitiven Elementes z besteht. Man arbeitet ausschließlich mit Werten, die entweder bekannt sind, wie p und v_p , oder mit solchen, die man leicht berechnen kann wie b, α oder w_p. Die *erste Teilaufgabe* lässt sich demnach so formulieren:

Gegeben ist eine Primzahl p und ein quadratischer Rest v_p (auch modulare Quadratzahl genannt) im endlichen Zahlenkörper Z_p . Gesucht sind die beiden Wurzeln ± s, welche die Gleichung

$$v_p = \pm s \text{ MOD } p$$

erfüllen. Dazu eignet sich der folgende Lösungsweg:

I. Überprüfung mit der Legendre-Formel, ob v_p wirklich ein quadratischer Rest in Z_p ist.

II. Wahl einer Zufallszahl r und Prüfung mit der Legendre-Formel, ob r ein nichtquadratischer Rest in Z_p ist. Wenn ja, dann w_p = r.

III. Zerlegung der Eulerzahl φ (p) = p-1 = 2^{α} ·b

IV. Berechnung von c = $v_p^{(b+1)/2}$ MOD p

V. Berechnung von d = w_p^{b} MOD p

VI. Setzen von i = 0

VII. Berechnung von x = c·d^{i} für i = 0, 1, 2, 3, ... 2^{α} - 1

VIII. Berechnung von x^2 MOD p

IX. Wenn x^2 MOD p = v_p ist, stellt x die eine Lösung, -x = p - x die andere dar → **Ende**

X. Wenn x^2 MOD p ≠ v_p ist, dann i = i + 1 gesetzt und Schritt VIII wiederholt.

Um die damit verbundenen Verhältnisse leichter verfolgen zu können, sind für den Fall p = 13, das primitive Element z = 2 und den nichtquadratischen Rest $w_p = 6 = z^5$ MOD 13 alle Lösungen in der Tabelle 4 mit den Potenzen des primitiven Elements dargestellt. Hier gilt wegen φ (p) = p - 1 = 12 = $2^2 \cdot 3$

$\alpha = 2$ b = 3.

Mit $s = z^i$ MOD 13 ist also

$v_p = z^{2i \text{ MOD } 12} \text{ MOD } 13,$

$c = v_p^{(b+1)/2} \text{ MOD } 13 = v_p^{2} \text{ MOD } 13 = z^{4i \text{ MOD } 12} \text{ MOD } 13$

$d = (z^5)^{b \text{ MOD } 12} \text{ MOD } 13 = z^{15 \text{ MOD } 12} \text{ MOD } 13 = z^3 \text{ MOD } 13.$

s	$z^{i\text{-Mod } 12}$	v_p = s^2 MOD 13 = $z^{2i \text{ MOD } 12}$ MOD 13	$c \cdot d^0$ = $v_p^{(b+1)/2}$ MOD 13 = $z^{4i \text{ MOD } 12}$ MOD 13	$c \cdot d^1$	$c \cdot d^2$	$c \cdot d^3$
1	$z^{12} = z^0$	z^0	***z^0***	z^3	z^6	z^9
2	z^1	z^2	z^4	z^7	z^{10}	***z^1***
3	z^4	z^8	$z^{16} = $ ***z^4***	z^7	z^{10}	z^1
4	z^2	z^4	z^8	z^{11}	***z^2***	z^5
5	z^9	$z^{18} = z^6$	$z^{12} = z^0$	z^3	z^6	***z^9***
6	z^5	z^{10}	$z^{20} = z^8$	z^{11}	z^2	***z^5***
7	z^{11}	$z^{22} = z^{10}$	$z^{22} = z^{10}$	***z^{11}***	z^2	z^5
8	z^3	z^6	$z^{12} = z^0$	***z^3***	z^6	z^9
9	z^8	$z^{16} = z^4$	***z^8***	z^{11}	z^2	z^5
10	z^{10}	$z^{20} = z^8$	$z^{16} = z^4$	z^7	***z^{10}***	z^1
11	z^7	$z^{14} = z^2$	z^4	z^7	z^{10}	z^1
12	z^6	$z^{12} = z^0$	z^0	z^3	***z^6***	z^9

Tabelle 4: Alle Lösungen zum Fall p = 13, z = 2 und $w_p = 6$ (Lösungen sind markiert)

Hier noch ein ***Hinweis*** zu primitiven Elementen in endlichen Zahlenkörpern**.**

Primitive Elemente z eignen sich zwar gut für theoretische Betrachtungen, haben aber für die praktische Verwendung meist keinen Wert, da es kein schnelles Verfahren zu ihrer Bestimmung gibt. Die Wahrscheinlichkeit, durch Wahl einer Zufallszahl auf ein primitives Element zu stoßen, wird mit wachsendem p sogar beliebig klein. Man weiß nur, dass es in einem Körper Z_p genau φ (p-1) verschiedene, wenn auch gleichwertige primitive Elemente gibt. Im Z_{13}, den wir bei einigen Beispielen verwendet haben, gibt es außer z = 2 noch die primitiven Elemente 6, 7 und 11, wobei 7 das zu 6, und 11 das zu 2 negative primitive Element darstellt.

Ein Beispiel aus einem etwas umfangreicheren Zahlenkörper soll zeigen, dass der Lösungsweg ganz allgemein brauchbar ist. Dazu wurde mit dem Miller-Rabin-Test eine Pseudoprimzahl p = 89633 bestimmt, die mit einer

Wahrscheinlichkeit von nur $4^{-10} \approx 10^{-6}$ keine Primzahl darstellt. Die Chance für 6 „Richtige“ im Lotto ist etwa 10^{-7}. Für $\varphi(p) = p-1 = 89632$ gilt die Zerlegung

$$\varphi(p) = p-1 = 2^5 \cdot 2801.$$

Also ist

$$\alpha = 5 \qquad b = 2801.$$

Durch Testen mit der Legendre-Funktion wurde der quadratische Rest

$$v_p = 51032$$

und der nichtquadratische Rest

$$w_p = 27756$$

gefunden. Die beiden Hilfsgrößen c und d sind demnach

$$c = v_p^{(b+1)/2} \text{ MOD } 89633 = 51032^{1401} \text{ MOD } 89633 = 20641$$

und

$$d = w_p^{b} \text{ MOD } 89633 = 27756^{2801} \text{ MOD } 89633 = 60784.$$

Für i = 0, 1, 2, 3, 4,... ergeben sich nacheinander die modularen Produkte

$$(c \cdot d^0 \text{ MOD } p)^2 \text{ MOD } p = (40301)^2 \text{ MOD } 89633 = 20641$$

$$(c \cdot d^1 \text{ MOD } p)^2 \text{ MOD } p = (75727)^2 \text{ MOD } 89633 = 38455$$

$$(c \cdot d^2 \text{ MOD } p)^2 \text{ MOD } p = (66519)^2 \text{ MOD } 89633 = 44316$$

$$(c \cdot d^3 \text{ MOD } p)^2 \text{ MOD } p = (35899)^2 \text{ MOD } 89633 = 84560$$

$$(c \cdot d^4 \text{ MOD } p)^2 \text{ MOD } p = (59064)^2 \text{ MOD } 89633 = 39736$$

$$(c \cdot d^5 \text{ MOD } p)^2 \text{ MOD } p = (75627)^2 \text{ MOD } 89633 = \mathbf{51032} \quad !$$

Mit s = 75627 ist damit die eine der beiden Wurzeln gefunden, die andere ergibt sich aus

$$-s \text{ MOD } p = (p-s) \text{ MOD } p = 89633 - 75627 = \mathbf{14006.}$$

Hier ist noch auf einen ***Sonderfall*** zu verweisen, mit dem man sich das Leben in der Hälfte aller Fälle besonders leicht machen kann. Wenn nämlich die Primzahl p MOD 4 = 3 ist, vereinfacht sich die Berechnung erheblich, da in diesen Fällen die Eulerzahl $\varphi(p) = p-1$ nur den Faktor 2 enthält, d. h. die Zerlegung von p-1 ergibt

$$p-1 = 2 \cdot b.$$

Wegen $\alpha = 1$ muss der oben angegebene Algorithmus also nur für i = 0 und i = 1 durchlaufen werden. Da für i = 1 aber die negative Wurzel herauskommt, bleibt nur noch die Bestimmung von

$$x = c \cdot d^{i} \text{ MOD } p = c \text{ MOD } p = v_p^{(b+1)/2} \text{ MOD } p = v_p^{(2b/2+1)/2} \text{ MOD } p$$

$$= v_p^{(2b/2+2/2)/2} \text{ MOD } p = v_p^{(2b+1+1)/4} \text{ MOD } p$$

$$= v_p^{(p+1)/4} \text{ MOD } p.$$

Zweite Teilaufgabe: *Algorithmus zur Bestimmung der modularen Quadratwurzeln in einer endlichen Restmenge mit dem aus einem Primzahlenprodukt n = p·q gebildeten Modul*

Wir wissen nun, wie man modulare Wurzeln berechnet, wenn der Modul eine Primzahl ist, für Primzahlenprodukte n = p·q ist hingegen kein direktes Verfahren bekannt. Hier hilft ein Zusammenhang zwischen den Resten bezüglich eines Produktmoduls n = p·q und den Resten zu den Primzahlmodulen p und q. Ist z. B. der Rest

$$v = s^2 \text{ MOD } n = s^2 \text{ MOD } (p \cdot q)$$

bekannt, so lassen sich daraus auch

$$v_p = s^2 \text{ MOD } p = v \text{ MOD } p$$

und

$$v_q = s^2 \text{ MOD } q = v \text{ MOD } q$$

berechnen. Der Wert s^2 muss selbst also gar nicht bekannt sein. Dies folgt aus der Definition für Reste:

$$v = s^2 \text{ MOD } n \quad \text{oder} \quad s^2 = i_n \cdot n + v = i_n \cdot p \cdot q + v$$

$$v_p = s^2 \text{ MOD } p \quad \text{oder} \quad s^2 = i_p \cdot p + v_p$$

$$v_q = s^2 \text{ MOD } q \quad \text{oder} \quad s^2 = i_q \cdot q + v_q.$$

Die Faktoren i_n, i_p und i_q sind darin geeignete eindeutige ganze Zahlen, welche die Gleichung erfüllen, die man allerdings nicht kennt, wenn s^2 unbekannt ist. Andererseits gilt:

$$v = s^2 - i_n \cdot n = s^2 - i_n \cdot (p:q) \text{ oder } v \text{ MOD } n = s^2 \text{ MOD } n = v$$

$$v \text{ MOD } p = s^2 \text{ MOD } p + i_n \cdot q \cdot p \text{ MOD } p = s^2 \text{ MOD } p + 0 = s^2 \text{ MOD } p$$

$$v \text{ MOD } q = s^2 \text{ MOD } p + i_n \cdot p \cdot q \text{ MOD } q = s^2 \text{ MOD } q + 0 = s^2 \text{ MOD } q.$$

Ein Vergleich mit

$$v_p = s^2 - i_p \cdot p \quad \text{oder} \quad v_p \text{ MOD } p = s^2 \text{ MOD } p = v \text{ MOD } p$$

$$v_q = s^2 - i_q \cdot q \quad \text{oder} \quad v_q \text{ MOD } q = s^2 \text{ MOD } q = v \text{ MOD } q$$

zeigt die Richtigkeit der oben getroffenen Annahme. Die im Authentikationsverfahren bekannte Zahl v stellt ihrerseits den quadratischen Rest zu s^2 bezüglich n dar. Also sind auch v_p und v_q quadratische Reste bezüglich p und q. Zu diesen wiederum können mit dem oben angegebenen Algorithmus die modularen Wurzeln zu den Zahlenkörpern Z_p und Z_q berechnet werden. Für das Beispiel aus dem Unterkapitel 5.10 waren folgende Zahlen gewählt worden:

$$p = 281, \quad q = 509, \quad n = p \cdot q = 143029.$$

Nehmen wir jetzt einmal an, dass wir die geheime Zahl s nicht kennen, sondern nur deren quadratischen Rest

$$v = s^2 \text{ MOD } n = 66291.$$

Dann ist

$$v_p = v \text{ MOD } p = 256$$

$$v_q = v \text{ MOD } q = 121.$$

(Mit der Kenntnis von s = 8133 hätten wir, wie erwartet, ebenfalls

$$v_p = s^2 \text{ MOD } p = 66145689 \text{ MOD } 281 = 256$$

$$v_q = s^2 \text{ MOD } q = 66145689 \text{ MOD } 509 = 121$$

erhalten. Aber wir kennen die Zahl s nicht).

Hierzu werden nun die modularen Wurzeln bestimmt. In diesem Fall ist dies besonders einfach, da die beiden quadratischen Reste zufällig Quadratzahlen kleiner als die Moduln p und q sind. Dies stellt aber keine Einschränkung dar, da wir andernfalls den oben behandelten Algorithmus benutzen würden. Wir haben also

$$s_p = \pm 16$$

$$s_q = \pm 11.$$

Die unbekannte Zahl s baut sich daraus gemäß Definition aus

$$s = i_p \cdot p + s_p$$

oder

$$s = i_q \cdot q + s_q$$

auf, wobei jedoch i_p bzw. i_q unbekannt sind. Man kann aber auf die erste Beziehung die MOD q -Funktion oder auf die zweite die MOD p -Funktion anwenden:

$$s \text{ MOD } q = s_q = (i_p \cdot p + s_p) \text{ MOD } q$$

$$s \text{ MOD } p = s_p = (i_q \cdot q + s_q) \text{ MOD } p.$$

Nach Umformung erhält man

$$i_p \cdot p \text{ MOD } q = (s_q - s_p) \text{ MOD } q$$

$$i_q \cdot q \text{ MOD } p = (s_p - s_q) \text{ MOD } p.$$

Dies ist je eine modulare lineare Gleichung in der Unbekannten i_p bzw. i_q, die anderen Größen sind alle gegeben.

Durch Multiplikation beider Seiten mit dem modularen inversen Element p^{-1} MOD q bzw. q^{-1} MOD p lassen sich die Gleichungen wie üblich nach den Unbekannten auflösen. Da p und q Primzahlen und damit teilerfremd sind, existieren auch die jeweiligen modularen Inversen. Es gilt

$$p^{-1} \cdot p \text{ MOD } q = 1$$

$$q^{-1} \cdot q \text{ MOD } p = 1$$

$$i_p \text{ MOD } q = p^{-1} \cdot (s_q - s_p) \text{ MOD } q$$

$$i_q \text{ MOD } p = q^{-1} \cdot (s_p - s_q) \text{ MOD } p.$$

Genau genommen sind damit aber nicht i_p bzw. i_q bekannt, sondern nur deren Reste bezüglich q bzw. p. Setzt man dies in die oben angegebenen Definitionsgleichungen für s ein, so ergibt sich mit einer ganzen - wiederum unbekannten - Zahl j_q bzw. j_p:

$$s = [j_q \cdot q + i_p \text{ MOD } q] \cdot p + s_p = j_q \cdot p \cdot q + (i_p \text{ MOD } q) \cdot p + s_p$$

$$= j_q \cdot n + (i_p \text{ MOD } q) \cdot p + s_p$$

$$s = [j_p \cdot p + i_q \text{ MOD } p] \cdot q + s_q = j_p \cdot p \cdot q + (i_q \text{ MOD } p) \cdot q + s_q$$

$$= j_p \cdot n + (i_q \text{ MOD } p) \cdot q + s_q.$$

Da bei der Bildung des modularen Quadrates $v = s^2$ MOD n jedoch alle Anteile mit n herausfallen, spielen sie keine weitere Rolle und es bleiben

$$s = (i_p \text{ MOD } q) \cdot p + s_p = [p^{-1} \cdot (s_q - s_p) \text{ MOD } q] \cdot p + s_p$$

$$s = (i_q \text{ MOD } p) \cdot q + s_q = [q^{-1} \cdot (s_p - s_q) \text{ MOD } p] \cdot q + s_q$$

Diese Bestimmungsgleichungen sind gleichwertig, so dass eine davon genügt. Erproben wir diese Ergebnisse nun mit dem begonnenen Beispiel, wobei als modulare Inverse ermittelt wurden:

p^{-1} MOD q = 413

q^{-1} MOD p = 53

Damit erhält man

s = [413·(11-16) MOD 509]· 281 + 16 = [413·504 MOD 509]·281 + 16 = 134896

oder

s = [53· (16-11) MOD 281]· 509 + 11 = [53·5 MOD 281]·509 + 11 = 134896.

Dieser Wert stellt die eine der beiden Wurzeln dar, die negative ergibt sich aus -s = (n - s) MOD n als

-s = 8133.

Beide Werte bilden dasselbe modulare Quadrat v, womit unsere Aufgabe gelöst ist.

Wenn die beiden Primzahlfaktoren p und q im Modul n bekannt sind, bietet das Fiat-Shamir-Verfahren also keine Sicherheit. Bei unbekannter Zerlegung ist die Sicherheit dagegen so hoch, wie es dem Aufwand für diese Zerlegung entspricht.