Karl Schwalen Juli 10 (Stand 1.20)

Weitere Aufsätze des Verfassers unter http://www.primath.homepage.t-online.de

Über quadratische Reste und quadratische Kongruenzen

(Mit zahlreichen Rechenbeispielen zur Lösung von Kongruenzen, der Berechnung des Jacobi-Symbols sowie zum Chinesischen Restsatz in den Anhängen)

Inhaltsübersicht

Ziffer	Thema	Seite
1.	Allgemeines bezügl. quadratischer Reste (QR) zu einem Primzahlmodul	2
2.	Spezielle Fragen	
2.a	Feststellen ob a ein QR zu einem nicht-primen Modul ist	2
2.b	Anzahl der QR im kleinsten pos. Vertretersystem	3
2.c	Abstände zwischen gleichen QR bei nicht-primen Moduln	5
2.d	Ist a ein QR zu einem Modul mit unbekannten Primteilern?	5
2.e	Beschreibung der QR durch Parabelsegmente	7
3.	Untersuchung zu den QR, die Quadratzahlen sind	
3.a	Positionen der QR im kleinsten pos. Vertretersystem	7
3.b	Ein Faktorisierungsverfahren („Spitzendetektor“)	10
4.	Untersuchungen im Hinblick auf das Quadratische Sieb	
4.a	„Innere“ Parabelsegmente, auf denen ausschließlich QR liegen	13
4.b	Anwendungen beim Quadratischen Sieb	17
	α) Der Siebvorgang	17
	β) Polynom-Wechsel	19
4.c	Zusammenfassung	21
Anhang 1		
I.	Lösen der quadratischen Kongruenz $x^2 \equiv a \bmod p$	1
II.	Lösen der qua. Kongruenz $x^2 \equiv a \bmod n$ (n zusammengesetzt)	4
Anhang 2		
I.	Lösen der Kongruenz $a \cdot x^2 + b \cdot x + c \equiv 0 \bmod n$	1
II.	Hensel-Lifting (Lösen von Kongruenzen höherer Ordnung)	3
III.	Beispiele zur Lösung allgemeiner Kongruenzen	5
IV.	Chinesischer Restsatz (System linearer Kongruenzen lösen)	7

1.Quadratische Reste zu Primzahlmoduln und deren Potenzen (Kurzübersicht)

Ist eine quadratische Kongruenz $\mathbf{x^2 \equiv a \bmod p}$ mit vorgegebenen Werten für a und p lösbar (d.h. es existiert eine ganze Zahl x, deren Quadrat bei Division durch p denselben Rest wie a lässt), wird a als quadratischer Rest (QR) bezeichnet, anderenfalls als quadratischer Nicht-Rest (QNR). Hierzu definiert man das Legendre-Symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 : a \text{ ist QR} \\ -1 : a \text{ ist QNR} \\ 0 : p \mid a \end{cases}$$

Die Frage der Lösbarkeit der o.a. Kongruenz ist im Fall 'p ist Primzahl > 2' durch das Quadratische Reziprozitätsgesetz völlig geklärt, und das Legendre-Symbol kann z.B. mit Hilfe des Euler-Kriteriums auch für große Zahlen schnell berechnet werden:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$$

Erwähnt sei noch, dass

- eine Quadratzahl natürlich zu jedem Modul p ein QR ist,
- es (p – 1) / 2 QR (Restklassen) gibt und ebenso viele QNR,
- eine primitive Restklasse kein QR ist,
- das Produkt zweier QR wiederum ein QR ist,
- für $p \equiv 3 \bmod 4$ folgt aus a ist QR(QNR): – a ist QNR(QR),
- für $p \equiv 1 \bmod 4$ folgt aus a ist QR(QNR): – a ist QR(QNR),
- aus a ist QR mod p folgt: a ist QR mod p^k für k = 2,3, ... (p > 2),
- für Moduln 2^k gilt: $k \le 2$: $a \equiv 1 \bmod 2^k$ ist QR; $k \ge 3$: $a \equiv 1 \bmod 8$ ist QR.

Wenn eine Kongruenz als lösbar erkannt ist, stellt sich als nächstes die Frage nach der Anzahl der Lösungen und wie man diese findet. Es gibt jeweils genau zwei Lösungen; ist x_1 eine Lösung, so lautet die andere Lösung $x_2 = -x_1$.

Für $p \equiv 3 \bmod 4$ erhält man eine Lösung als $x_1 \equiv a^{\frac{p+1}{4}} \bmod p$. Der Fall $p \equiv 1 \bmod 8$ ist wesentlich aufwendiger und (bisher) nur rekursiv lösbar. Der entsprechende sog. Tonelli-Algorithmus ist (mit den Alg. zum schnellen Potenzieren sowie zur Berechnung des Legendre-/Jacobi-Symbols) im **Anhang 1** dargestellt.

(Auch für Moduln p^k mit k > 1 kennt man gut handhabbare Lösungsverfahren. Stichwort: Hensel-Lifting; siehe **Anhang 2**)

2. Spezielle Eigenschaften der QR

2.a Quadratische Reste zu einem nicht-primen Modul n

Die QR bilden eine Untergruppe der primen Restklassengruppe zum betr. Modul. Daher kann eine Zahl a nur dann QR sein, wenn ggT(a, n) = 1 ist. Beispiel: Die primen Restklassen zum Modul 12 sind: 1, 5, 7, 11 ($\varphi(12) = 4$). Wegen $1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \bmod 12$ ist die Restklasse 1 der einzige QR zum Modul 12.
Wie man feststellt, ob a QR zu einem Modul ist, dessen Primfaktorzerlegung bekannt ist, siehe Beispiele 1 und 2 im **Anhang 1**.

Im weiteren ist (wenn nicht ausdrücklich etwas anderes gesagt wird) der Modul n stets eine Primzahl oder eine Zahl, die das Produkt zweier Primzahlen ist; also $n = p \cdot q$.
Bei bekannten Faktoren p und q ist die Kongruenz $x^2 \equiv a \bmod n$ lösbar, genau dann, wenn a ein QR modulo p und modulo q ist. Ist die Lösbarkeit gegeben, sind zunächst die Kongruenzen zu den (primen) Moduln p und q wie unter 1.gezeigt zu lösen; für die so erhaltenen vier Lösungspaare ergeben sich mittels Chinesischem Restsatz vier Lösungen, die der Ausgangskongruenz genügen (siehe Beispiel 3 im **Anhang 1**).
Zwei davon (z.B. x_1 u. x_2) liegen in jedem Fall im Bereich $0 < x \leq (n-1)/2$; die beiden anderen erhält man im kleinsten positiven Restesystem aus $x_3 = n - x_1$ und $x_4 = n - x_2$ bzw. im absolut kleinsten Restesystem als $-x_1$ und $-x_2$.
Das rührt daher, weil wegen $(n - x)^2 \bmod n = (n^2 - 2nx + x^2) \bmod n = x^2 \bmod n$ das System der QR zur Gerade $x = n / 2$ und wegen $x^2 \bmod n = (-x^2) \bmod n$ zur Nullachse ($x = 0$) symmetrisch ist. Daher braucht man immer nur die Eigenschaften dieses „Halbsystems“ zu untersuchen, in dem $0 < x \leq (n - 1) / 2$ gilt.

2.b Anzahl der QR im kleinsten pos. Vertretersystem

Im nachstehenden Bild 1 sind die QR beispielhaft für die Primzahl 137 dargestellt, wobei die einzelnen Werte zur besseren Übersicht in der Reihenfolge ihres Auftretens durch Gradenstücke verbunden sind. Jeder QR kommt in dem Halbsystem genau einmal vor, was gleichbedeutend damit ist, dass die Kongruenz $x^2 \equiv a \bmod p$ für $0 < x \leq (p - 1) / 2$ genau eine Lösung besitzt.

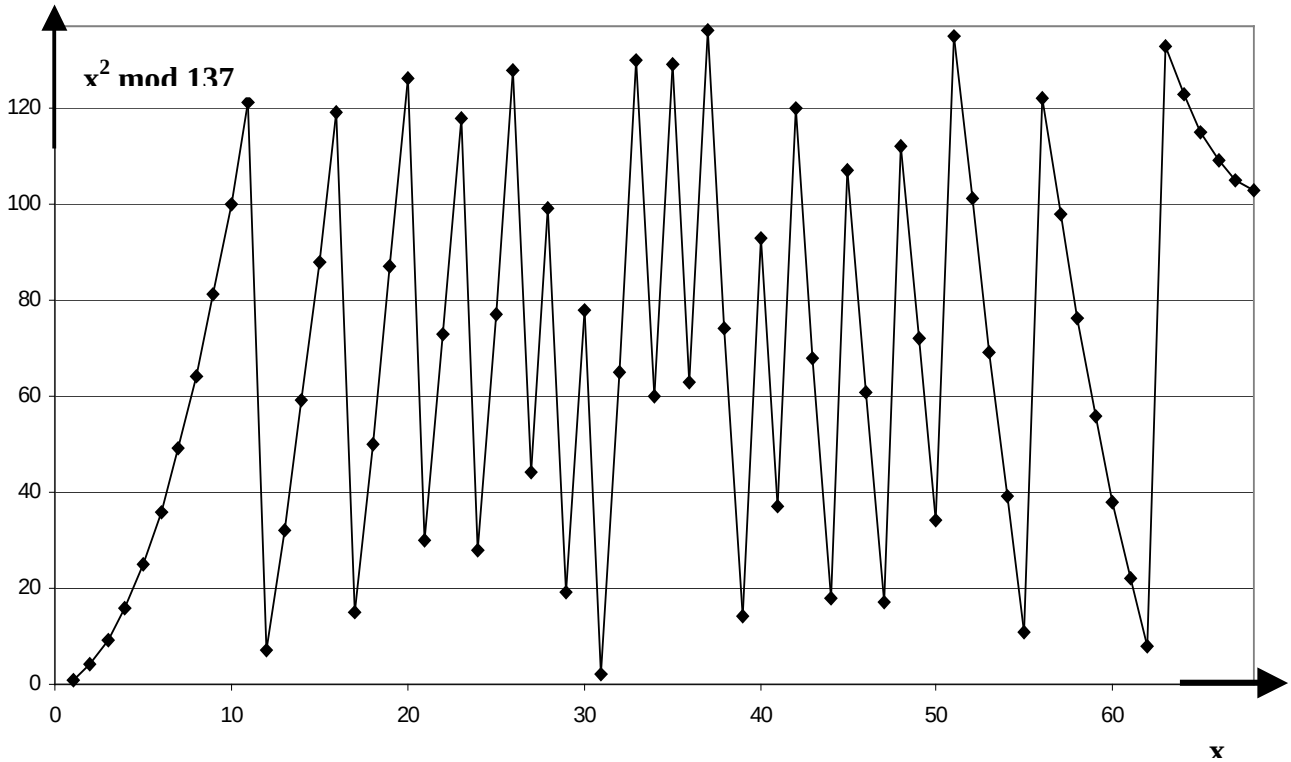


Bild 1: Darstellung der QR modulo der Primzahl 137 für $0 < x \leq (n - 1)/2$

In der Zahlentheorie wird allgemein bewiesen, dass die Anzahl der QR modulo einer Primzahl p gleich $\varphi(p) / 2$, also gleich $(p - 1) / 2$ ist, wobei $\varphi(n)$ die EULER’sche Funktion bedeutet.

Wählt man dagegen einen Modul n, der das Produkt zweier Primzahlen ist, ist als erstes zu berücksichtigen, dass die Zahlen a mit $a = x^2 \bmod n$, für die ggT(a, n) > 1 gilt, keine QR sind. Die Anzahl N_g dieser Zahlen im Halbsystem lässt sich wie folgt angeben:

$$N_g = \left\lfloor \frac{n-1}{2p} \right\rfloor + \left\lfloor \frac{n-1}{2q} \right\rfloor = \frac{n-1}{2} - \frac{\varphi(n)}{2} = \frac{n-1}{2} - \frac{(p-1)\cdot(q-1)}{2} = \frac{p+q-2}{2}$$

Wie oben bereits erwähnt, besitzt eine quadratische Kongruenz im Fall $n = p \cdot q$ im Bereich $0 < x \le (n-1)/2$ genau zwei Lösungen, d.h. jeder QR kommt zweimal vor. Damit erhält man: $N_{QR} = \left(\frac{n-1}{2} - N_g\right)/2 = \frac{(p-1)\cdot(q-1)}{4} = \frac{\varphi(n)}{4}$ (Gilt so nur für $n = p \cdot q$!)

In Bild 2 ist der Verlauf von $x^2 \bmod 133$ ($= 7 \cdot 19$) wiedergegeben, wobei Reste mit $ggT(x^2 \bmod 133, 133) > 1$ sowie die QR, die (nicht-triviale) Quadratzahlen sind, farbig markiert sind.

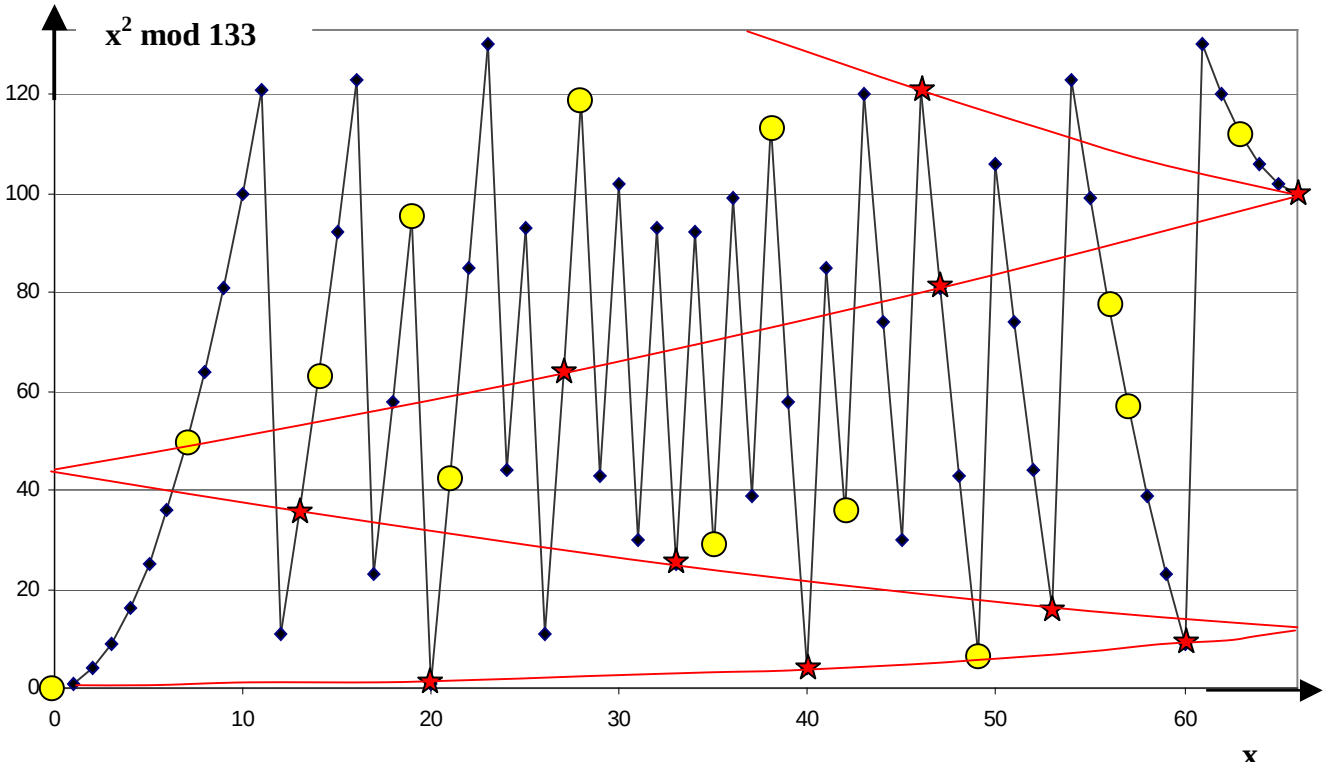


Bild 2: Darstellung der QR modulo 133 (= 7 · 19) (im Halbsystem)

: kein quadr. Rest, da ggT > 1 : Quadr. Rest ist Quadratzahl (x > Wurzel n)

(Die rote Linie wird weiter unten erläutert.)

2.c Abstände zwischen gleichen QR bei einem nicht-primen Modul

Hat man zu einem beliebigen QR die zwei Lösungen x_1 , x_2 ($0 < x_1, x_2 \leq (n-1)/2$) gefunden, lassen sich die beiden Faktoren p und q bekanntlich mittels $ggT(x_1 - x_2, n)$ und $ggT(x_1 + x_2, n)$ bestimmen. Die Differenz zwischen beiden Lösungen ist also immer ein Vielfaches von p oder von q.
Nun bereitet es ja keine Schwierigkeiten, zu einen beliebigen x den zugehörigen QR zu finden: Man muss nur x^2 mod n ausrechnen. Das Problem der Teilersuche besteht also einzig darin, die ***zweite*** (inkongruente) Lösung der betr. quadr. Kongruenz zu bestimmen.

In Bild 2 sind für die QR, die Quadratzahlen sind, die jeweiligen „zweiten“ Lösungen gekennzeichnet. (Die „erste“ Lösung ist in diesen Fällen trivial: $a^2 = x_1^2$.) Es wird deutlich, dass die Abstände zwischen den beiden Lösungen regellos verteilt sind – abgesehen davon, das sie Vielfache des einen oder des anderen Teilers sind. In Bild 3 wird die Problematik für die QR, die keine Quadratzahlen sind, visualisiert.

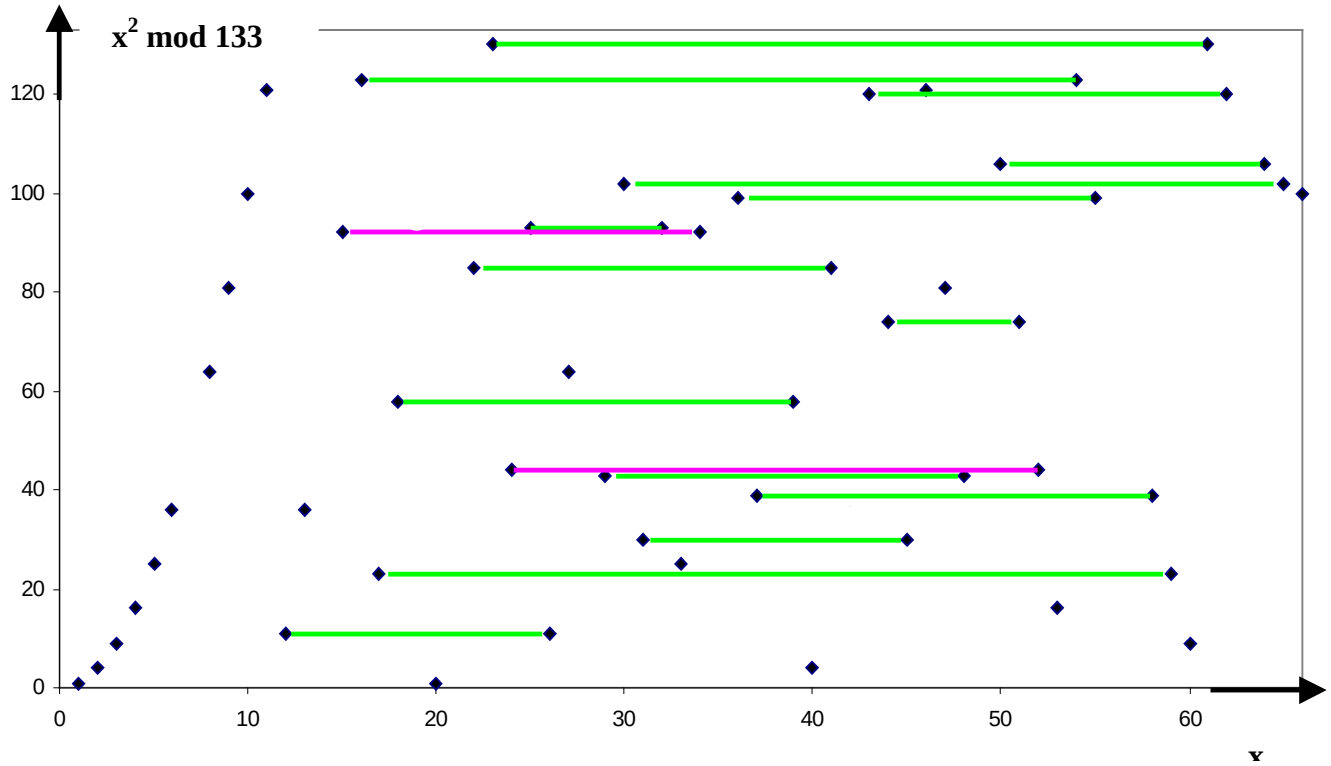


Bild 3: n = 133; Kennzeichnung der Abstände gleicher QR (, die keine Quadratzahlen sind)

2.d Prüfung, ob a ein QR modulo eines n mit unbekannter Primfaktorzerlegung ist

Zur Entscheidung dieser Frage kann (für ungerades n) zunächst das Jacobi-Symbol befragt werden. Ist das Ergebnis $\left(\frac{a}{n}\right) = -1$, steht fest, dass a kein QR ist. Hat dagegen das Jacobi-Symbol den Wert 1, lässt sich daraus nur folgern, dass a mit einer gewissen Wahrscheinlichkeit ein QR ist, denn wenn $\left(\frac{a}{p}\right) = -1$ und $\left(\frac{a}{q}\right) = -1$, hat das ebenfalls $\left(\frac{a}{p \cdot q}\right) = 1$ zum Ergebnis. Also:

Sei n eine (ungerade) zusammengesetzte, große Zahl mit unbekannter Primfaktorzerlegung und a (keine Quadratzahl), so dass ggT(a, n) = 1 und $\left(\frac{a}{n}\right)$=1.

Dann kann (abgesehen man findet zufällig ein x, für das x^2 mod n = a ist) nicht entschieden werden, ob a ein QR modulo n ist.

(„große Zahl“ bedeutet vorstehend, dass es (aufgrund des Zeitbedarfs) praktisch nicht möglich ist, für alle x mit $0 < x \leq (n - 1) / 2$ die Werte von x^2 mod n darauf zu prüfen, ob der Wert a sich darunter befindet.)

Ist die zur Prüfung vorgelegte Zahl klein, kann eine andere Strategie verfolgt werden: Bekanntlich erhält man im Zusammenhang mit der Kettenbruchentwicklung von $\sqrt{n}$ ausschließlich QR, die betragsmäßig kleiner als $2\sqrt{n}$ sind. Führt man für mehrere dieser QR eine Zerlegung in die Primfaktoren durch, lassen sich meist einzelne Primfaktoren als QR nachweisen - und evtl. ist die vorgelegte Zahl unter ihnen.

<u>Beispiel:</u> Es seien (im System der absolut kleinsten Reste) die folgenden QR gegeben:

1813 ; – 3996; – 3441; 6600; 1034

$1813 = 7^2 \cdot 37$ ==> 37 ist QR
$-3996 = 2^2 \cdot 3^3 \cdot 37$ ==> – 3 ist QR
$-3441 = -3 \cdot 31 \cdot 37$ ==> 31 ist QR
$6600 = 2^3 \cdot 3 \cdot 5^2 \cdot 11 = 2^2 \cdot (-3) \cdot 5^2 \cdot (-11 \cdot 2)$ ==> – 22 ist QR
$1034 = 2 \cdot 11 \cdot 47 = -22 \cdot (-47)$ ==> – 47 ist QR

Das ist allerdings ein recht mühsames Verfahren.

Erwähnt sei noch, wie in „halb-trivialer“ Weise quadr. Reste konstruiert werden können, ohne x^2 mod n auszurechnen und für die die Lösung der quadratischen Kongruenz sich ohne weiteres angeben lässt. Ausgangspunkt ist die Beobachtung, dass $((n - 1) / 2)^2$ mod n im Fall $n \equiv 3 \bmod 4$ den QR (n +1) / 4 liefert und für $n \equiv 1 \bmod 4$ den QR (3·n + 1) / 4. Das lässt sich verallgemeinern zu der Regel:
Sei $1 < m < \sqrt{n}$ eine natürliche Zahl mit ggT(m, n) = 1 sowie r = n mod m und $v = n \bmod m^2$. Dann ist

$$\left(\frac{n-r}{m}\right)^2 \bmod n = \left(\frac{n^2 - 2nr + r^2}{m^2}\right) \bmod n = \frac{n \cdot (n \bmod m^2) - 2nr + r^2}{m^2} = \frac{n \cdot (v - 2r) + r^2}{m^2} = a$$

Der Term (v – 2r) ist stets als kleinster positiver Rest mod m^2 einzusetzen.
<u>Beispiel:</u>

n = 1.234.567 m = 4 → r = n mod 4 = 3; v = n mod 16 = 7 → v – 2r = 1 →

$a = (n \cdot 1 + 3^2) / 4^2 = 77.161$; $x = (n - 3) / 4 = 308.641$ → $x^2 \bmod n = a$

Zahlen dieser ‘Bauart’ werden weiter unten noch eine Rolle spielen.

2.e Parabelsegmente und „Spitzenwerte“

Hinweis: $y = \lfloor x \rfloor$ bedeutet hier: y ist die größte ganze Zahl < x (Abrundung falls x > 0)

Die Parabel $y = x^2$ wird durch den Operator ’mod n’ in das kleinste pos. Restesystem reduziert. Dabei bleiben von der ursprünglichen Parabel mehr oder weniger lange zusammenhängende Stücke erhalten (wie sie z.B. in Bild 1. deutlich zu erkennen sind).
Den x–Wert, an dem das k-te Parabelsegment endet, erhält man aus $x^2 = k \cdot n$ zu $\mathbf{x_k = \lfloor \sqrt{k \cdot n} \rfloor}$. Der zugehörige QR ist im kleinsten pos. Restsystem x_k^2 mod n („obere Spitze“ qr_{ko}). Erhöhen von x_k um 1 führt auf die „untere Spitze“ (des k + 1-ten Parabelsegmentes: $qr_{ku} = (x_k + 1)^2 \bmod n = qr_{ko} + 2 \cdot x_k + 1 - n$.
Die x_k stellen allerdings nur „Spitzenwerte“ dar, solange x nicht viel größer als n / 4 ist, denn dann ist der Abstand zwischen x^2 und $(x + 1)^2 > n$.
Hinsichtlich der Spitzen im Bereich $n / 4 < x < n / 2$ kann man sich zunutze machen, dass wegen der Symmetrieachse x = n / 2 eine weitere einfache Parabel existiert, die vermittels des Operators ’mod n’ alle QR erzeugt, und zwar in der genau umgekehrten Reihenfolge wie bei der Berechnung mit x^2 mod n. Diese Funktion – in der Variablen h geschrieben – ist

$$(h^2 - h + t) \bmod n \quad \text{mit} - (n-1)/2 < h \le 0 \text{ und } t = \begin{cases} (n+1)/4 & \text{für } n \equiv 3 \bmod 4 \\ (3n+1)/4 & \text{für } n \equiv 1 \bmod 4 \end{cases}$$

Werden die gesuchten Spitzen beginnend bei (n – 1) / 2 mit f nummeriert, ergibt sich unter Berücksichtigung von x = (n – 1) / 2 – h :

$$x_f = \frac{n-1}{2} - \left\lfloor \left(\sqrt{n \cdot (4f - s)} - 1\right) / 2 \right\rfloor \quad \text{mit } s = \begin{cases} 1 & \text{für } n \equiv 3 \bmod 4 \\ 3 & \text{für } n \equiv 1 \bmod 4 \end{cases}$$

und die obere Spitze zu $qr_{fo} = x_f^2 \bmod n$ sowie $qr_{fu} = (x_f - 1)^2 \bmod n = qr_{fo} - 2 \cdot x_f + 1$.

Schließlich sei noch angegeben, wie viele dieser relativen Maxima bzw. genau so viele rel. Minima es gibt: Deren Anzahl ist für $n \ge 7$ im Bereich $< (n - 1) / 2$: $\lfloor (n+3)/8 \rfloor$.

Mit Hilfe der o.a. Formeln ist es auch möglich die Anzahl z_k der QR im k-ten Parabelsegment zu berechnen:
$z_k = x_k - x_{k-1} = \lfloor \sqrt{k \cdot n} \rfloor - \lfloor \sqrt{(k-1) \cdot n} \rfloor$. Möchte man im umgekehrten Fall ein Parabelsegment mit einer vorgegebenen Anzahl von QR untersuchen, ergibt sich die zugehörige Nummer des Parabelsegments zu $k \approx \left(\frac{n - z_k^2}{2 \cdot z_k \cdot \sqrt{n}} \right)^2$ und daraus x_k. Diese Formel kann man auch für die Parabelsegmente im Bereich zwischen n/4 und n/2 benutzen, wobei k dann ausgehend von (n – 1) / 2 gezählt wird.

3. Untersuchung zu den QR, die Quadratzahlen sind

3.a Die Verteilung der Quadratzahlen im System der kleinsten pos. QR

Für $x < \sqrt{n}$ ist $x^2 \bmod n = x^2$. Diese x-Werte nennt man aus ersichtlichem Grund die „trivialen“ Wurzeln der Quadratzahlen. Ist n eine Primzahl gibt es – wie eingangs erwähnt – keine weiteren QR, die Quadratzahlen sind. Im weiteren ist wieder $n = p \cdot q$ und für diesen Fall soll untersucht werden, inwieweit die Verteilung der nichttrivialen Wurzeln der Quadratzahlen beschrieben werden kann.

Das Interesse an diesen Wurzeln der Quadratzahlen ist klar: Verfügt man über ein solches x_1 mit $x_1^2 \bmod n = a^2$, kann mittels $ggT(x_1 - a, n)$ sofort ein Teiler von n bestimmt werden.

Im nachstehenden Bild 4 sind die betr. x-Werte mit $x^2 \bmod n = a^2$ (Zahlen unterhalb der Balken), für $n = 203 = 7 \cdot 29$ sowie – zwischen den Balken – deren Abstände untereinander eingetragen.

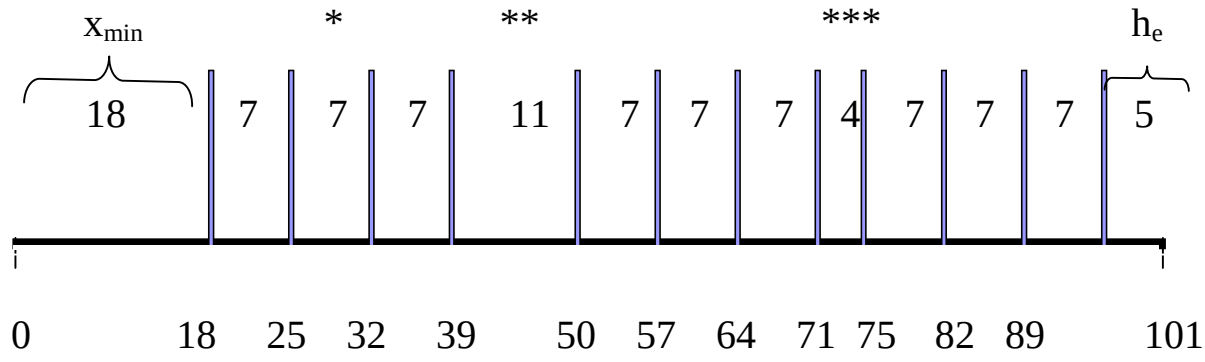


Bild 4: Verteilung der (nichttrivialen) Lösungen von $x^2 \equiv a^2 \bmod n$ für $n = 7 \cdot 29$ und $1 < a < \sqrt{n}$ im Bereich $0 < x \leq (n-1)/2$

Da aus den Wurzeln von a^2 die Teiler einer Zahl bestimmt werden können, sollte die Abhängigkeit zwischen Wurzeln und Teiler sich auch formelmäßig beschreiben lassen.
In der Tat gelten folgende Formeln (wobei stets q > p angenommen ist):

- Abstand des kleinsten x ($x > \sqrt{n}$) mit $x^2 \bmod n = a^2$ vom Punkt Null

$$x_{min} = \frac{q-p}{2} + k \cdot p \quad \text{mit } k = \left\lfloor \frac{\sqrt{q/p} + 3}{2} - \sqrt{q/p} \right\rfloor \qquad (q/p < 5{,}82 \dashrightarrow k = 1)$$

- Kleinster Abstand h_e vom Punkt $(n-1)/2$ (s. Bild 4.)
  - $n \equiv 3 \bmod 4$

$$h_{e3} = \frac{q-p-2}{4} + k_3 \cdot p \quad \text{mit } k_3 = \left\lfloor \frac{\sqrt{q/p} + 5}{4} - \sqrt{q/p} \right\rfloor \qquad (q/p < 13{,}92 \dashrightarrow k_3 = 0)$$

  - $n \equiv 1 \bmod 4$

$$h_{e1} = \frac{|q-3p|-2}{4} + k_1 \cdot p \quad \text{mit } k_1 = \left\lfloor \frac{\sqrt{q/p} + 7}{4} - \sqrt{q/p} \right\rfloor \qquad (q/p < 9 \dashrightarrow k_1 = 0)$$

- Abstände d der Quadratzahlen im Bereich zwischen x_{min} und h_e (Bezeichnungen siehe Bild 4.)

$$*: \quad d_* = p \qquad **: \quad d_{**} = \frac{q-p}{2} \qquad ***: \quad d_{***} = \frac{|q-3p|}{2}$$

Generell werden alle vorkommenden Abstände der nichttrivialen Lösungen aller möglichen Kongruenzen $x^2 \equiv a^2 \bmod n$ im Bereich $\sqrt{n} < x \leq \frac{n-1}{2}$ durch die o.a. Formeln wiedergegeben (experimenteller Befund !).
Die Abstände d_{**} und d_{***} kommen zusammen insgesamt genau $(p-3)/2$ - mal vor. Da die

Anzahl der Quadratzahlen im betrachteten Bereich mit $\lfloor\sqrt{n}\rfloor - \lfloor\frac{\sqrt{n}}{p}\rfloor$ anzugeben ist, lässt sich auch die Anzahl der Abstände d_* (= p) ausrechnen.
Aus den Formeln für x_{min} und h_e erkennt man, dass die Quadratzahlen über den gesamten Bereich $\sqrt{n}$ bis $\frac{n-1}{2}$ verteilt sind, wenn p und q etwa gleich groß sind; ist dagegen p sehr viel kleiner als q, werden die Quadratzahlen auf einen immer kleineren Bereich eingeengt. x_{min} strebt dabei gegen den Grenzwert q. Ein (extremes) Beispiel: $n = 3 \cdot 37813 = 113439$
Es ist dann $x_{min} = 37478$ und $(n-1)/2 - h_{e3} = 38147$. Wegen $(3-3)/2 = 0$ kommen die Abstände d_{**} und d_{***} nicht vor, und die 223 Abstände $d_* = 3$ füllen die Lücke $38147 - 37478 = 669$ genau aus. In diesem Bereich ergibt sich also für jedes dritte x: $x^2 \bmod n = a^2$.

Bemerkenswert ist noch folgendes: Der ganzzahlige Term $k = \left\lfloor \frac{q/p + 3}{2} - \sqrt{q/p} \right\rfloor$ hängt nicht etwa von der jeweiligen Zahl n, sondern nur vom Teilerverhältnis q / p ab. So ist für q / p < 5,828.. k = 1, für q / p < 9 ist k = 2 usw. Daher kann x_{min} offenbar nicht jeden beliebigen Wert annehmen. Um zu sehen, wo diese „verbotenen“ Bereiche liegen, werden weitere Gleichungen benötigt:
Die Auflösung der vorstehenden Gleichung für k nach $v_s^* = q_s^* / p_s^*$ ergibt $v_s^* = (1+\sqrt{2\cdot(k-1)})^2$. Die Kennzeichnung mit * soll darauf hinweisen, dass es sich bei q und p hier nicht um die beiden Teiler einer bestimmten Zahl n handelt, sondern um ’laufende’ Größen, wobei der Index s daran erinnert, dass der Wert sich nicht kontinuierlich ändert, sondern „springt“, wenn k um 1 erhöht wird.

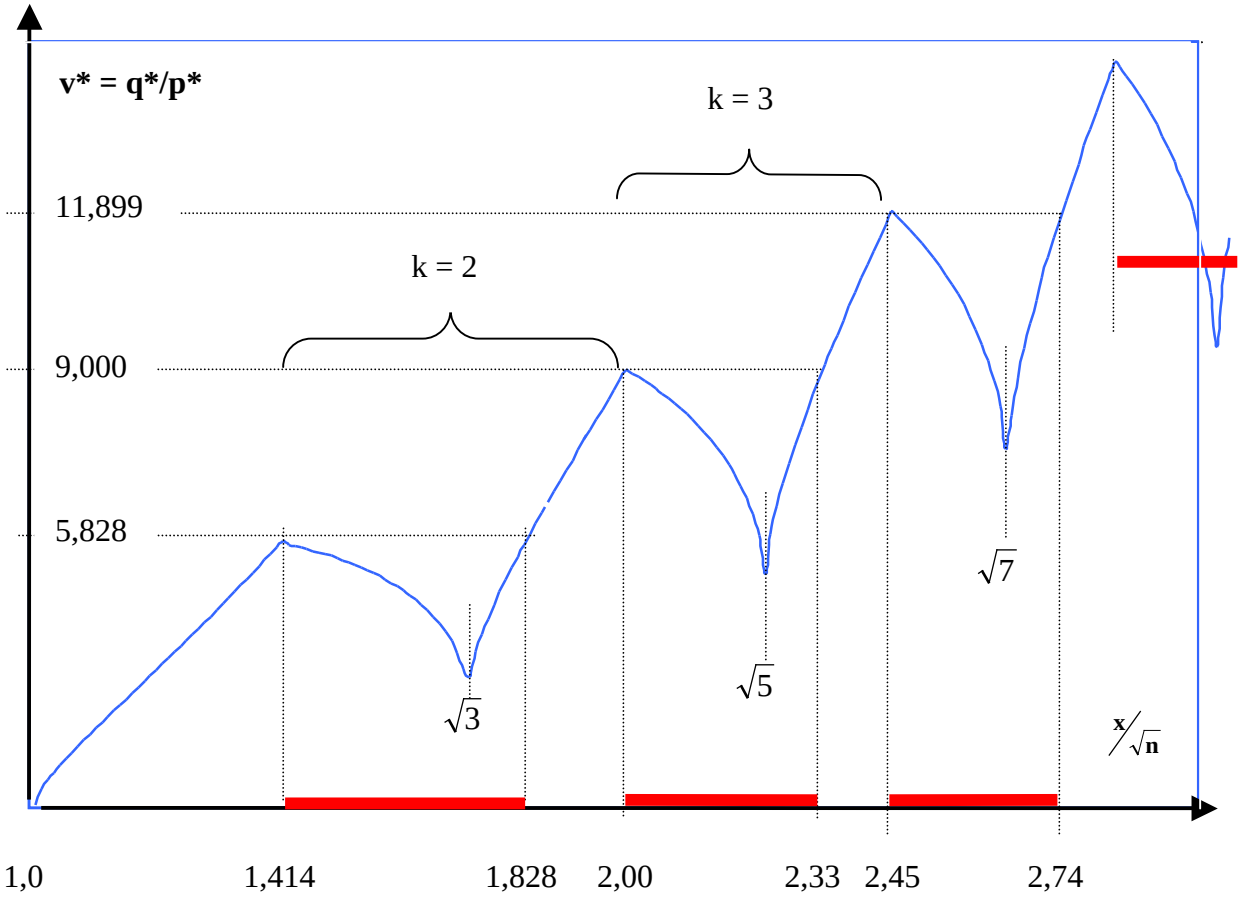


Bild 5. Erläuterung im Text

Mit Hilfe der allgemeinen Beziehungen q = v · p und p = $\sqrt{n/v}$ erhält man für den Beginn der jeweiligen Sprungstellen als Funktion von k die erstaunlich einfache Beziehung:

$x_s(k) = \sqrt{n} \cdot \sqrt{2 \cdot (k-1)}$ und als 'Sprungweite': $\Delta_x(k) = \sqrt{n} \cdot \left(\frac{1}{1+\sqrt{2 \cdot (k-1)}}\right)$

Die Abhängigkeit des laufenden Teilerverhältnisses v^* von x und k ist gegeben durch

$$\mathbf{v^*(x,k) = \frac{\left(\sqrt{|\,x^2 - n \cdot (2k-3)\,|} + x\right)^2}{n}}$$

Diese Funktion ist in Bild 5 als blauer Kurvenzug dargestellt, wobei auf $\frac{x}{\sqrt{n}}$ normiert wurde.

Der Graph beschreibt den Zusammenhang zwischen v^* und dem kleinsten x-Wert bei dem $(x_{min})^2$ mod n eine Quadratzahl ist. Z.B. befindet sich im Bereich $\sqrt{n} < x < \sqrt{2} \cdot \sqrt{n}$ mindestens eine Quadratzahl, wenn das Teilerverhältnis q / p < 5,828 ist.

In den rot markierten Bereichen findet sich x_{min} nie, und der Grund dafür ist infolge des Verlaufs des Graphen klar: In diesen Bereichen liegen ausschließlich Teilerverhältnisse v^*, die bereits mit kleineren x-Werten erreicht wurden. Hätte die betr. Zahl n ein solches v^* besessen, wäre x_{min} eben beim erstmaligen Auftreten fixiert worden.
Am rechten Ende des Bereichs (Werte von h_e; siehe obige Formeln) liegen die Verhältnisse analog.

3b. Quadratsuche an den unteren Spitzen / Ein Faktorisierungs-Verfahren

Die Differenz zwei aufeinanderfolgender, auf demselben Stück der Parabel $f(x) = x^2 - k \cdot n$ $(0 < f(x) < n)$ befindlicher QR beträgt 2x + 1. Daraus folgt, dass alle hinreichend kleinen, nichttrivialen Quadratzahlen als erste Zahl dieser Parabelstücke zu finden sind – also an den hier im Hinblick auf die graphische Darstellung so bezeichneten 'unteren Spitzen'. Entsprechend wurde vorliegend keine ungerade Zahl (mit zwei Primteilern) gefunden, bei der mehr als eine Quadratzahl $< 4 \cdot \sqrt{n}$ nicht eine solche Position besetzt hätte.

Während im vorhergehenden Punkt untersucht wurde, bei welchem x die erste Quadratzahl auftritt, soll nun versucht werden, die zwangsweise Häufung der Quadratzahlen an den unteren Spitzen zur Teilersuche zu nutzen.

Die durchgeführten Untersuchen erbrachten folgenden Zusammenhang:

Sei n = q· p und v = q / p > 1 das Teilerverhältnis.
$\left(\left\lfloor \sqrt{k \cdot n} \right\rfloor + 1\right)^2 \bmod n$ ist eine Quadratzahl, wenn die Zahl k ein Teilerpaar (o, u) besitzt mit o ≥ u und o ≡ u mod 2, für das mit v^* = o / u die Ungleichung gilt:

$$\mathbf{v^* - \frac{2 \cdot \sqrt{2} \cdot o^{3/4}}{\sqrt[4]{n} \cdot u^{5/4}} < v < v^* + \frac{2 \cdot \sqrt{2} \cdot o^{3/4}}{\sqrt[4]{n} \cdot u^{5/4}}}$$

Beispiel: n = 1777· 421 = q· p; q / p = 4,2209....

Die obige Ungleichung erfüllt k = 39 = 13· 3 = o· u; o / u = 4,3333....

denn es ist 4,1665... < 4,2209.... < 4,5001....

Also ist $(\lfloor\sqrt{39\cdot n}\rfloor+1)^2 \bmod n$ eine Quadratzahl. (In der Tat ist $5041 = 71^2$.)

Der kleinste Wert von k = o·u hängt demnach davon ab, ob der Bruch q / p sich durch einen Näherungsbruch o / u mit relativ kleinem Zähler und Nenner im Rahmen der vorstehenden Ungleichung approximieren lässt.
Von zwei Zahlen gleicher Größenordnung dürfte z.B. die erste Quadratzahl in der Regel früher zu finden sein, wenn $v \approx 8$ ist, als wenn $v \approx \pi$ ist.
Wegen $o \equiv u \bmod 2$, ist $k_{min} \neq 2b$ (b ungerade Zahl) ; außerdem ist $k_{min} \neq 4b$, da man anderenfalls immer kürzen kann. Somit: Das zu einem k_{min} gehörende v^* ist stets ein voll gekürzter Bruch und für ein gerades k_{min} gilt: $8 \mid k_{min}$.

Bemerkenswert am obigen Ergebnis ist vor allem, dass allein aus der Kenntnis der Primfaktorzerlegung von k die näherungsweise Bestimmung eines Teilerpaars von n möglich ist – ohne Zuhilfenahme der betr. Quadratzahl.

Nachfolgend der auf den obigen Ergebnissen basierende Faktorisierungs-Algorithmus:

Eingabe: n (ungerade, kleinster (echter) Teiler > $n^{1/3}$)

---

a = 0: vn = 10080 * n: r = 1: w = 0
Do while w^2 <> r
    a = a + vn: x = isqrt(a)
    r = (x + 1)^2 – a: w = isqrt(r)
Loop
t1 = ggT(x + 1 – w, n): t2 = n / t1

Ausgabe: t1, t2 ist ein Teilerpaar von n

Zweck und Wirkung des Vorfaktors 10080 sind im Beitrag „Das Fermat-Verfahren und das Lehman-Verfahren“ auf der Netz-Seite des Verfassers ausführlich dargestellt. Dort ist auch aufgezeigt, wie der o.a. Alg. für Teiler < $n^{1/3}$ ertüchtigt werden kann. Der Alg. ist im Mittel um einen Faktor > 3 schneller als das sog. Lehman-Verfahren.
In dem Alg. wird anstelle von $\left(\lfloor\sqrt{k\cdot n}\rfloor+1\right)^2 \bmod n$ mit $\left(\lfloor\sqrt{k\cdot n}\rfloor+1\right)^2 - k\cdot n$ gerechnet, was eine rekursive Berechnung gestattet. Die beiden Ausdrücke sind allerdings nur im Bereich k < n / 4 gleichwertig. Die detektierten Quadratzahlen liegen nur im Bereich k < n / 16 an den ‚unteren Spitzen’ (im Sinne der graphischen Darstellung).
Das dargestellte Verfahren, das sich noch in mancherlei Hinsicht beschleunigen lässt, wobei es allerdings die ‚Einfachheit’ einbüßt, ist für Zahlen bis etwa 28 Dezimalstellen brauchbar.

Die Durchmusterung der unteren Spitzen auf der rechten Seite des Halbsystems gestaltet sich etwas aufwendiger. Es gilt dort (s.o.) für die f-te Spitze: $x_f = \frac{n-1}{2} - \lfloor (\sqrt{n \cdot (4f - s)} - 1) / 2 \rfloor$
Damit erhält man den folgenden Algorithmus:

Eingabe: n (ungerade, kleinster (echter) Teiler > $n^{1/3}$)
---
s = (n + 2) Mod 4: h = (n – 1) / 2: r = 1: f = 1
Do while w^2 < > r
    fn = (4 * f – s) * n: y = Int ((Sqrt (fn) – 1) / 2)
    x = h – y – 1: r = x^2 Mod n : w = isqrt (r) : f = f + 1
Loop
t1 = ggT(x – w, n): t2 = n / t1

Effizienzsteigerung mittels Vorfaktor (wie z.B. 10080) ist hier nicht möglich.

Die folgenden Ausführungen behandeln im Wesentlichen die Möglichkeit im System der quadratischen Reste Parabeln zu definieren, deren Punkte ausschließlich quadratische Reste sind und diese Parabeln im Hinblick auf mögliche Anwendungen im Rahmen des Faktorisierungsverfahren „Quadratisches Sieb“ zu nutzen.

4. Überlegungen zum Quadratischen Sieb

Vorbemerkung:
Bei großen Zahlen (z.B. mit 80 oder 100 Dezimalstellen) ist die direkte Suche nach einer modularen Wurzel aus einer Quadratzahl mit Ausnahme von Sonderfällen ein völlig aussichtsloses Unterfangen. Wesentlich effektiver ist die beim Kettenbruchverfahren und insbesondere beim Quadratischen Sieb (QS) verfolgte Strategie, ein (inkongruentes) Zahlenpaar (x, y), das die Kongruenz $x^2 \equiv y^2 \bmod n$ erfüllt, auf indirektem Weg zu finden, nämlich geeignete QR zu multiplizieren, so dass ihr Produkt eine Quadratzahl ist. Zur Feststellung der Eignung eines QR ist dessen Faktorisierung notwendig, was man mittels des sog. quadratischen Siebes (daher der Name) bewerkstelligt, das seinerseits auf dem bekannten Satz „ $a \equiv b \bmod p \rightarrow f(a) \equiv f(b) \bmod p$“ beruht. Insbesondere folgt daraus für das Siebpolynom: $f(x + k \cdot p) \equiv f(x) \bmod p$. Zur Berechnung der für die Siebung mit den einzelnen p_i erforderlichen Startwerte werden zunächst die Lösungen $\pm x_1$ von $x^2 \equiv n \bmod p$ ermittelt.
Bei der Basis-Variante des QS wird als Polynom zur Generierung der QR $f(x) = (x + w)^2 - n$ verwendet, wobei $w = \lfloor \sqrt{n} \rfloor$. Um genügend QR zu finden, die über der sog. Faktorbasis ‚FB' (das ist die Menge der Primzahlen p_i unterhalb einer Schranke B, für die $\left(\frac{n}{p_i}\right) = 1$ sowie die Zahlen –1 und 2) zerfallen, arbeitet man beim „MPQS“ mit einer Vielzahl von Siebpolynomen. Diese „synthetisiert“ man folgendermaßen:

Gegeben sei ein quadratische Polynom $f(x) = a \cdot x^2 + b \cdot x + c$ für dessen Koeffizienten gilt: $b^2 - 4a \cdot c = n$. Dann gilt auch $4a \cdot f(x) = (2a \cdot x + b)^2 - n$. Allerdings muss bei jedem Polynomwechsel das „Sieb“ neu justiert werden, was bedeutet, für jedes p_i der FB ist die lineare Kongruenz $2ax + b \equiv \pm y_p \bmod p$ zu lösen, wobei die beiden (für die FB einmalig zu berechnenden) y_p die Lösungen von $y^2 \equiv n \bmod p$ (s.o.) sind.
Die Lösung der lin. Kongr. ist $x_{1,2} = (\pm y_p - b) \cdot (2a)^{-1} \bmod p$; d.h. 2a muss bei jedem Polynomwechsel für jedes p_i invertiert werden, was Zeit kostet und zur Entwicklung des „SIQS“ führte, bei dem man a (in diesem Fall das Produkt einiger Primzahlen der FB) konstant hält, und nur b geändert wird. Die konkreten Werte für b müssen $b^2 \equiv n \bmod a$ genügen und diese Kongruenz besitzt 2^k Lösungen, wenn a in k Primfaktoren zerfällt. (siehe Anhang 2)

Der vorstehende kurze Überblick soll zeigen, dass die Betrachtung von Parabeln, die ausschließlich QR darstellen, durchaus von „praktischem“ Interesse sein kann.

4.a Parabelvarianten / „Innere“ Parabeln, auf denen ausschließlich QR liegen

In der „Definitionsgleichung“ $a = y^2 \bmod n$ kann y eine beliebige ganzzahlige Funktion f(x) sein. Im einfachsten Fall ist f(x) = x. Eine naheliegende Verallgemeinerung ist wohl $f(x) = s_o \cdot x$, mit einer Konstanten s_o. Für x = 1 ist dann $r_o = s_o^2 \bmod n$ und somit ergibt sich die QR–Folge: $a = (r_o \cdot i^2) \bmod n$ mit i = 1, 2, 3,.... Soll x – wie hier vereinbart – auf das Halbsystem beschränkt werden, berechnet man x aus
$x = (s_o \cdot i) \bmod n$ und falls das Ergebnis größer als n / 2 ist, wird x durch n – x ersetzt. Der folgend Alg. erzeugt also alle QR, die aber je nach Wahl von s_o gegenüber der ‚natürlichen' Reihenfolge beliebig umgeordnet sind.

```
Eingabe: n, s_o <  g = (n – 1)/ 2
---------------------------------
 For i = 1 to g
        x = (s_o* i) mod n: if x > g then x = n – x
        a = x^2 mod n
Next i
```

Hinsichtlich der Beschaffung kleiner, leicht zerlegbarer QR lassen sich aus dieser „Umordnung“ im Allgemeinen keine Vorteile gegenüber der Wahl $s_o = 1$ erkennen. Interessant ist noch der Fall $r_o = s_o^2 \bmod n = 1$ ($s_o > 1$; genau dieses s_o ist bei einem Faktorisierungs-Problem natürlich nicht bekannt): Dann durchläuft die Folge der QR zunächst alle Quadratzahlen kleiner $\sqrt{n}$ (siehe roten Kurvenzug in Bild 2) und insgesamt ergibt sich eine zu $s_o = 1$ identische Folge der QR; für alle quadratischen Kongruenzen sind lediglich „intern“ (in der Reihenfolge bzw. der graphischen Darstellung) die Plätze der beiden Lösungen vertauscht.

„Innere“ Parabeln, auf denen ausschließlich QR liegen

In Ziffer 2. wurde bereits erwähnt, dass nicht nur $f(x) = x^2 \bmod n$ für $0 < x \leq (n-1) / 2$ einen kompletten „Satz“ QR zum Modul n liefert, sondern auch $f(y) = y^2 – y + ((n – 1) / 2) \bmod n$ für $– (n – 1) / 2 < y \leq 0$. Die Scheitel (0, 0) bzw. (1 / 2, ((n – 1) / 2) mod n –1 / 4) der beiden Parabeln liegen auf den beiden (einzigen) Symmetrie-Achsen (x = 0 und x = n / 2) und der Funktionswert ist im zweiten Fall nicht ganzzahlig.
Wie aus dem unten stehenden Bild 6 ersichtlich, gibt es innerhalb der durch $x^2 \bmod n$ gebildeten QR-Folge eine Vielzahl von Verläufen, bei denen die QR augenscheinlich in Parabelform angeordnet sind. Drei derartige Verläufe sind als Beispiele rot markiert.
Ziel dieses Abschnittes ist die Beschreibung dieser Parabeln.

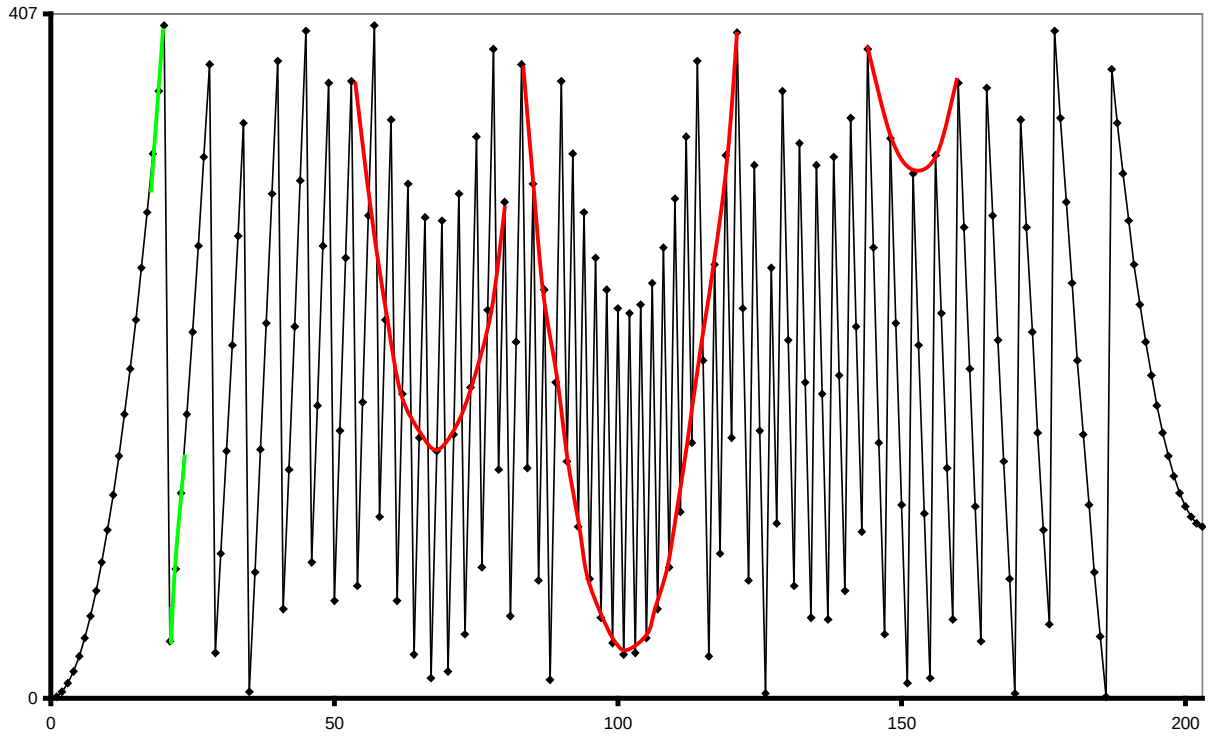


Bild 6: QR-Folgen in Parabelform am Beispiel n = 407 (= 11·37)

Die zwischen dem Scheitelpunkt a_e dieser Parabeln und n liegenden QR (hier mit a_y bezeichnet) durch

$$\mathbf{a_y = s^2 \cdot y^2 + (2 \cdot s \cdot e - g) \cdot y + a_e} \qquad \mathbf{(*)}$$

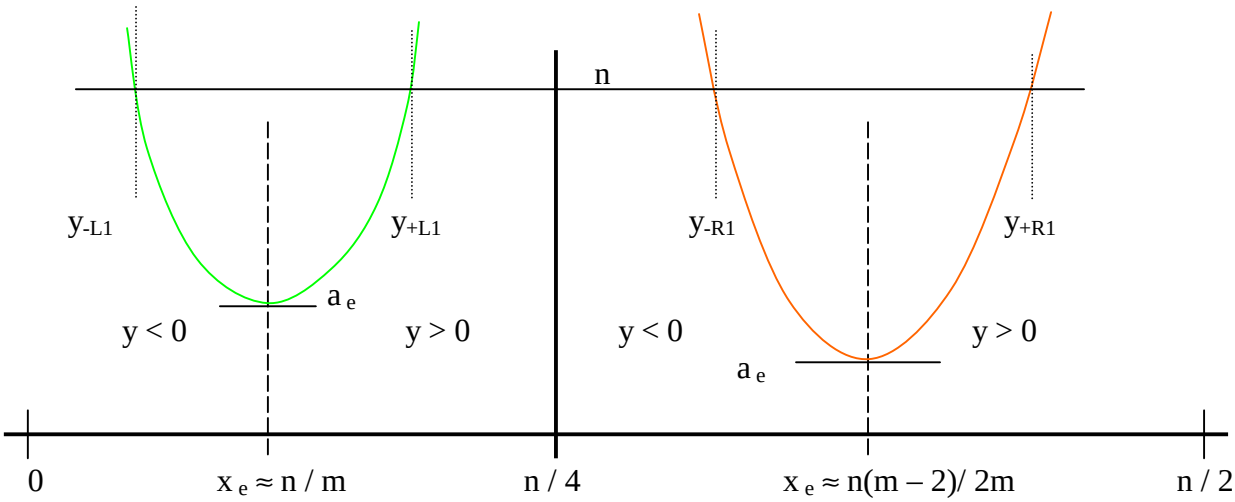
beschrieben.
Die Werte von s, g und a_e sind durch die Vorgabe der zwei Größen m und e festgelegt, wobei für jedes Paar (m, e) für $m > 2$ je eine Parabel im linken und im rechten Teil des Halbsystems liegt (siehe unten).

Vorgabe: nat. Zahl **m** mit $1 \le m < \sqrt{n}$.

Vorgabe: nat. Zahl **e** in den Grenzen
- m gerade: $-(m-2) \operatorname{div} 4 \le e \le m \operatorname{div} 4$
- m ungerade: $-(m-1)/2 \le e \le (m-1)/2$

Bestimmung der weiteren Konstanten:

linker Teil des Halbsystems (HS)	**rechter Teil** des Halbsystems (HS)
m gerade: $s = m/2$ $g = r$ m ungerade: $s = m$ $g = 2 \cdot r$	m gerade: $s = m/2$ $v = (m-2)/2$ m ungerade: $s = m$ $v = m-2$
$r = n \bmod m$ (falls $r > m/2$ und zugleich $m \neq 0 \bmod 4 \rightarrow r = r - m$)	$g = (v \cdot n) \bmod (2 \cdot s)$ (falls $g > s$ und zugleich $m \neq 0 \bmod 4 \rightarrow g = g - 2s$)
$x_0 = \frac{n-r}{m}$	$x_0 = \frac{v \cdot n - g}{2 \cdot s}$
Scheitelpunkt $(x_e; a_e)$: $x_e = x_0 + e$;	$a_e = x_e^2 \bmod n$



Die Anzahl der für einen Wert von m möglichen Werte von e gibt an, wie viele Parabeln ‚ineinander gestapelt' sind, wobei deren Scheitelpunkt-Ordinaten x_e jeweils um ± 1 gegeneinander versetzt sind.
Die Umrechnung der „lokalen" Koordinate **y** in die Koordinate **x** geschieht über
$x = x_0 + e + s \cdot y$.
(Wenn m eine gewisse Größe übersteigt, kommt es für die betragsmäßig größeren Werte von e zu Überlappungen mit den durch den nächstgrößeren Wert m + 1 und e bestimmten

Parabeln; d.h. es gibt Mehrfachdarstellungen. Die Grenze m_g ab dem das vorkommt, erhält man näherungsweise aus der Bedingung
$\frac{n}{m+1}+\frac{m}{4} > \frac{n}{m}-\frac{m}{2}$ zu $m_g \approx \sqrt[3]{4 \cdot n/3}$. Im Bereich $m \approx \sqrt{n}$ ergeben sich nur noch für e = 0 neue Parabeln.)

Für m = 1 und e = 0 ergibt (*) richtigerweise $a_y = y^2$ (x = y) und für m = 2 , e = 0:
$a_y = y^2 - y + (n-1)/2)^2 \bmod n$ wobei dieser Sonderfall zum linken HS gehört.

Bild 7 verdeutlicht die Verhältnisse bezüglich der e-Werte nochmals am konkreten Beispiel.

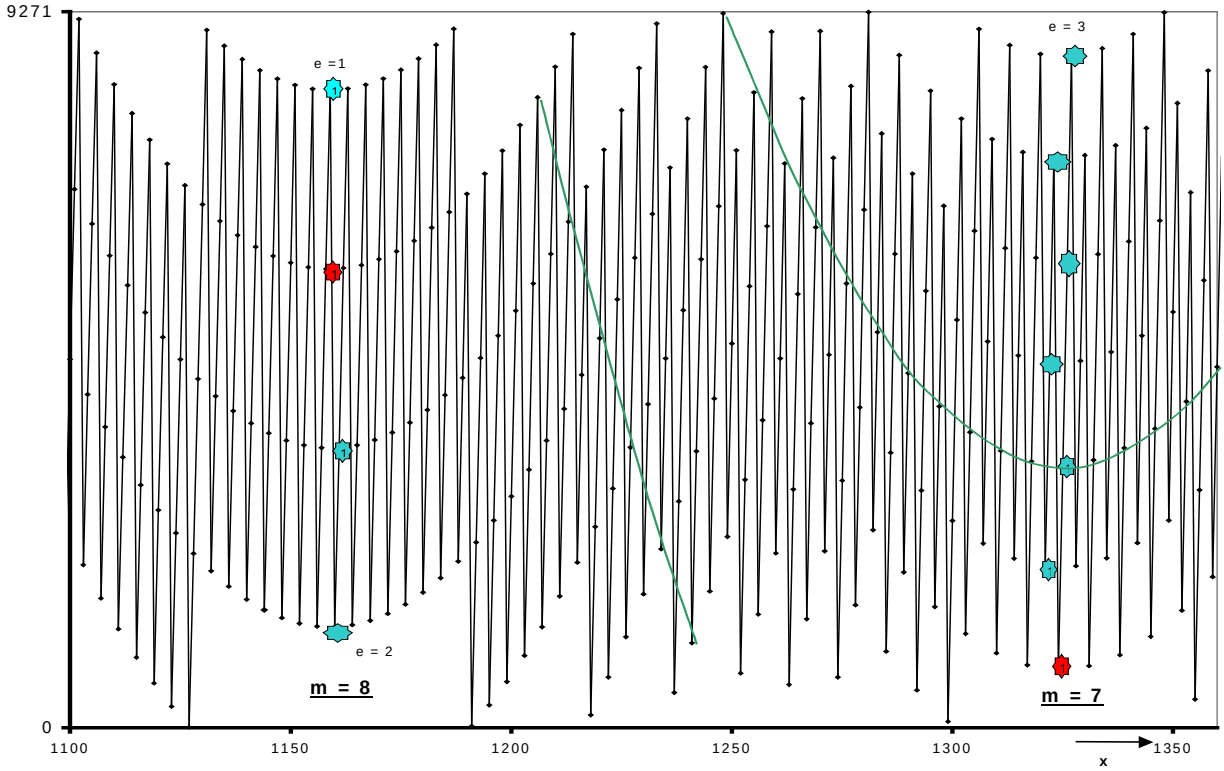


Bild 7: n = 9271; Detailansicht der QR für m = 7 und m = 8
Rote Punkte: e = 0; türkis: e ≠ 0
Grüne Kurve: Beispiel für m = 7 und e = 1 (linker Teil des HS)

Die Koeffizienten der markierten Kurve (m = 7, e = 1) sind gemäß den o.a. Rechenschritten:

r = 3; s = 7; g = 6; $x_0 = 1324 \rightarrow s^2 = 49$; 2se – g = 8; $a_e = (x_0+1)^2 \bmod n = 3406 \rightarrow$
$a_y = 49 \cdot y^2 + 8 \cdot y + 3406$

4.b Anwendbarkeit der o. a. QR-Folgen beim Quadratischen Sieb

Um mit der o.a. Parabelgleichung betragsmäßig kleinste QR in der Umgebung von n zu erhalten, ist – bei geeigneter Wahl von y – jeweils n bzw. allgemeiner k·n abzuziehen, so das damit gilt

$a_y = s^2 \cdot y^2 + (2 \cdot s \cdot e - g) \cdot y + a_e - k \cdot n$ mit $a_e = (x_o + e)^2 \bmod n$;

$x = x_o + e + s \cdot y$; s, g, e und x_o gemäß den o.a. Definitionen und unter Benutzung der üblichen Abkürzungen $a = s^2$; $b = 2se - g$; $c = a_e - k \cdot n$ und $d_k = b^2 - 4ac$

$$\mathbf{a_y = a \cdot y^2 + b \cdot y + c}$$

Bei Anwendungen wird meist k = 1 sein, also $c = a_e - n$ und $d_k = d_1$; dies wird im weiteren einfach mit ‚**d**' bezeichnet.
Zur Bestimmung der 'geeigneten' Werte von y ist die Festlegung des Siebintervalls [– H, H] Voraussetzung. An den Grenzen des Siebintervalls ist $a_y = \pm H$. Die Auflösung der quadratischen Gleichung nach y ergibt bekanntlich für den rechten Ast (y > 0):

$$y_{R\pm H} = \left\lfloor \frac{1}{2a} \left(-b + \sqrt{d \pm 4a \cdot H} \right) \right\rfloor$$

Des weiteren ist $y_{L\pm H} \approx - y_{R\pm H}$, da – b / 2a meistens kleiner 1.

α) Der Siebvorgang

Es bestehen folgende Kongruenzen: $(s \cdot y + x_e)^2 \equiv a \cdot y^2 + b \cdot y + c \mod n$ (∗)
und $(2 \cdot a \cdot y + b)^2 \equiv 4 \cdot a(a \cdot y^2 + b \cdot y + c) \mod n$ (∗∗)
Voraussetzung für (∗∗) ist $d = d_e \cdot n$. Das ist bei der hier vorgenommenen Bestimmung der Parabel-Koeffizienten „**automatisch**" erfüllt (siehe unter β).
Die zur Faktorbasis gehörenden p_i (Berechnung $(\frac{d}{p_i})$) sowie die Siebkongruenzen werden in der üblichen Weise ermittelt: Lösen von $t^2 \equiv d \bmod p_i \rightarrow \pm t_1$ und dann Lösen von $2a \cdot y + b \equiv \pm t_1 \bmod p_i$. Mit den (im 'Normalfall' $t_1 \neq 0$) zwei Lösungskongruenzen $y_{1,2}$ gilt nun für alle y: für $\mathbf{y \equiv y_{1,2} \bmod p_i \rightarrow p_i \mid a_y}$ Auf das Siebintervall bezogen, heißt das: p_i teilt im Siebintervall den QR a_y für alle $y = y_u + y_{1,2} - r + k \cdot p_i$ (mit $r = y_u \bmod p_i$ und $y_{1,2}$ als kleinste pos. Reste; k = 0, 1, 2,..). Durch Anwendung des Hensel-Lifting kann das Sieb auch für höhere Potenzen der p_i verfeinert werden.
Klarerweise lassen sich beide Parabel-Äste (y < 0 bzw. y > 0)mit der gleichen Siebeinstellung bearbeiten.
Die – etwa nach dem Logarithmus-Kriterium – für eine vollständige Zerlegung über der Faktorbasis anstehenden QR sowie die zugehörigen x-Werte werden zweckmäßigerweise mittels (∗) ausgerechnet. Werden – etwa um die höheren Potenzen der p_i herausdividieren zu können – von vornherein alle a_y innerhalb des Siebintervall berechnet, kann ausgenutzt werden, das zwischen den QR a_y (rechter Ast) und a_{-y} (linker Ast) die Beziehung $a_{-y} = a_y - 2b \cdot y$ besteht.
(Bezüglich der Vorgehensweise zum Lösen quadratischer und linearer Kongruenzen sowie zum Hensel-Lifting siehe **Anhänge 1 und 2)**

Nachstehend ein „handliches" Beispiel, an dem – unter Benutzung einer der in Bild 7 veranschaulichten Parabeln (m = 8, oberste Parabel) – der Siebvorgang und das abschließende Lösen der Legendre-Kongruenzen dargestellt wird.

n = 9271 (= 73·127) m = 8 e = 1 → a = 16 b = 1 c = – 1014 d = 64.897
Als FB werden die Primzahlen < 30 gewählt, für die es Lösungen von $t^2 \equiv d \bmod p_i$ gibt.

	$t^2 \equiv d \bmod p_i$	$2a\cdot y + b \equiv \pm t_1 \bmod p_i$
p_i	**$t_{1,2}$**	**$y_{1,2}$**
2	1	0
3	±1	0, 2
7	0	5
13	±1	0, 4
17	±12	3, 15 = – 2
29	±16	4, 5

$x_0 = 1158$ s = m / 2 = 4

Das Siebintervall sei [– 1020, 600]. Somit liegt der Scheitelpunkt im Siebintervall, was den Siebvorgang besonders anschaulich macht.

y	**a_y**	**– 1**	**2**	**3**	**7**	**13**	**17**	**29**	**Zerlegung**	**x = x_0 + e + s·y**	**Bez.**
–10	576		×	×					$2^6 \cdot 3^2$	1119	(a)
– 9	273			×	×	×			3·7·13	1123	(b)
– 8	2		×						2	1127	(c)
– 7	– 237	×		×							
– 6	– 444	×	×	×					$-2^2 \cdot 3 \cdot 37$	1135	(d)
– 5	– 619	×									
– 4	– 762	×	×	×							
– 3	– 873	×		×							
– 2	– 952	×	×		×		×		$-2^3 \cdot 7 \cdot 17$	1151	(e)
– 1	– 999	×		×					$-3^3 \cdot 37$	1155	(f)
0	**– 1014**	×	×	×		×			$-2 \cdot 3 \cdot 13^2$	1159	(g)
1	– 997	×									
2	– 948	×	×	×							
3	– 867	×		×			×		$-3 \cdot 17^2$	1171	(h)
4	– 754	×	×			×		×	– 2·13·29	1175	(i)
5	– 609	×		×	×			×	– 3·7·29	1179	(j)
6	– 432	×	×	×					$-2^4 \cdot 3^3$	1183	(k)
7	– 223	×									
8	18		×	×					$2 \cdot 3^2$	1191	(l)
9	291			×							
10	596		×						x : Startwerte der Siebung		

Folgende QR-Produkte ergeben Quadratzahlen und man erhält echte Teiler von n:

(a): (QR ist Quadrat) $a_y = (2^3 \cdot 3)^2$ → $\mathbf{1119}^2 \equiv \mathbf{24}^2 \bmod n$ ggT(1119 – 24, 9271) = 73

(c)·(l): $(1127 \cdot 1191)^2 \equiv \mathbf{7233}^2 \equiv (18)\cdot(2) \equiv \mathbf{6}^2 \bmod n$ ggT(7233 – 6, 9271) = 127

(h)(k): $(1171 \cdot 1183)^2 \equiv \mathbf{3914}^2 \equiv (-867)\cdot(-432) \equiv (2^2 \cdot 3^2 \cdot 17)^2 \equiv \mathbf{612}^2 \bmod n$
ggT(3914 – 612, n) = 127

(d)·(f): $(1135 \cdot 1155)^2 \equiv \mathbf{3714}^2 \equiv (-444)\cdot(-999) \equiv (2 \cdot 3^2 \cdot 37)^2 \equiv \mathbf{666}^2 \bmod n$
ggT (3714 – 666, n) = 127

(c)·(g)·(h): $(1171 \cdot 1159 \cdot 1127)^2 \equiv \mathbf{3881}^2 \equiv (2)\cdot(-1014)\cdot(-867) \equiv (2 \cdot 3 \cdot 13 \cdot 17)^2 \equiv \mathbf{1326}^2 \bmod n$
ggT(3881 – 1326, n) = 73

(b)·(c)·(i)·(j): …..

β) Polynom-Wechsel

Voraussetzung für einen Polynom-Wechsel ist, dass die Faktorbasis unverändert weiter benutzt werden kann, was wiederum bedeutet, dass die Diskriminante d für alle Polynome gleich bleibt.
Beim MPQS bewerkstelligt man das durch geschickte Änderungen der Größen a, b (und c). Da vorliegend die Koeffizienten a, b und c (und somit auch d) im wesentlichen durch die Wahl von m festgelegt werden, sind demnach hier Regeln gefragt, welche m-Werte die gleichen Diskriminante d nach sich ziehen.
Dazu ist als erstes der Zusammenhang zwischen d_e ($d = d_e \cdot n$) und m darzustellen.

m gerade; (f = 0, 1,...,m / 2 – 1)

rechte Seite des HS	linke Seite des HS
I. $d_e = n \bmod (2m) + f \cdot 2m + (k-1) \cdot m^2$	**II: $d_e = r + f \cdot 2m + (k-1) \cdot m^2$**
(Der Term $(k-1) \cdot m^2$ besagt, dass d_e ab k = 2 bei jedem „Nulldurchgang" von a_y um m^2 zunimmt. Die Laufvariable f ersetzt hier e, was die Formeln sehr vereinfacht.)	Zur Bestimmung von r sind drei Fälle zu unterscheiden, wobei als ‚Startwert' stets **$r = n \bmod (2m)$** dient. 1. $m \equiv 2, 6 \bmod 8$ – $m / 2 \equiv 1 \bmod 4 \rightarrow r = r - m / 2$ – $m / 2 \equiv 3 \bmod 4 \rightarrow r = r + m / 2$ Ist nun $r \leq 0 \rightarrow r = r + 2m$ $r > 2m \rightarrow r = r - 2m$ 2. $m \equiv 4 \bmod 8$ Ist $r < m / 2 \rightarrow r = r + 2m$ 3. $m \equiv 0 \bmod 8$ Falls $r < m \rightarrow r = r + m$ $r > m \rightarrow r = r - m$

m ungerade; (f = 0, 1,....., m – 1)

III: $d_e = 4 \cdot (n \bmod m + f \cdot m + (k-1) \cdot m^2)$	**IV: $d_e = r + 4 \cdot (f \cdot m + (k-1) \cdot m^2)$** (Die Berechnung von r ist zu unübersichtlich weshalb die Darstellung hier unterbleibt.)

Für gerades m (und k = 1, was im weiteren stets angenommen wird) gilt also $0 < d_e < m^2$; für ungerades m: $0 < d_e < 4m^2$.
Da n ungerade ist, ist d_e im Fall I. immer ungerade; im Fall III. ist der Klammerausdruck für gerades f ebenfalls ungerade und II. 2. und 3. ergeben auch ein ungerades d_e. (Im Fall IV. ist d_e ungerade, wird jedoch nicht weiter benützt, da zu komplex.)
Somit ist klar, dass bei ungeradem n ein vorgegebenes d_e ungerade sein muss, wenn man möglichst zahlreiche m-Werte finden will, die auf die gleiche Diskriminante führen.
Nun ist in III. der Klammerausdruck zwar ungerade, d_e wegen des Faktors 4 aber grade.

Das lässt die Faktorbasis aber unverändert, da eine Quadratzahl zu jedem teilerfremden Modul ein QR ist, also $\left(\frac{d}{p_i}\right) = \left(\frac{4\cdot d}{p_i}\right)$. Allerdings hat $t^2 \equiv d \bmod p_i$ andere Lösungen als $t^2 \equiv (4d) \bmod p_i$ und muss daher – für jedes p_i einmalig – zusätzlich berechnet werden.

Aus der o.a. Tabelle lassen sich die notwendigen Bedingungen für „brauchbare" Werte von m leicht ablesen, und die experimentellen Befunde zeigen, dass diese im wesentlichen auch bereits hinreichend sind. Es gilt nämlich:
Unter Beachtung von $m > \sqrt{d_e}$ (siehe obige Ungleichung für d_e) gibt es zu einem vorgegebenen d_e geeignete m-Werte, die gestatten a, b und c so zu berechnen, dass $b^2 - 4ac = d_e \cdot n$, wenn die folgenden Bedingungen erfüllt sind:

- Fall I. $(m \equiv 0 \bmod 2)$: $2m \mid (n - d_e)$
- Fall III. $(m \equiv 1 \bmod 2)$: $2m \mid (n - d_e)$ $\quad (d = 4 \cdot d_e \cdot n)$
- Fall II. 2. $(m \equiv 4 \bmod 8)$: $m \mid (n - d_e)$
- Fall II. 3. $(m \equiv 0 \bmod 8)$: $m \mid (n - d_e)$ und zugleich $(n - d_e) \bmod 2m = m$

Die Anzahl der brauchbaren m-Werte hängt also von den Teilbarkeitseigenschaften der Zahl $n - d_e$ ab.
Daher bietet sich folgende einfach zu realisierende Vorgehensweise an: Man wählt eine Zahl Π, die das Produkt (ausreichend) vieler kleiner Primzahlen ist (etwa $\Pi = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot ....$) und setzt $d_e = n \bmod \Pi$. Dann ist $n - d_e = \Pi \cdot (n \operatorname{div} \Pi)$. So kann die Anzahl der zur Verfügung stehenden m-Werte nahezu beliebig gewählt werden.
Diese Vorgehensweise hat allerdings einen gravierenden Nachteil: Je größer die Diskriminante, desto kleiner ist die Anzahl N_{QR} der im vorgegebenen Siebintervall aufzufindenden QR, was wiederum nur (zeitintensiv) durch eine Vergrößerung des Intervalls oder zusätzliche Polynomwechsel kompensiert werden kann.
Formelmäßig lässt sich die Abhängigkeit N_{QR} von m, d_e und H einfach darstellen:
H sei als Vielfaches von $\sqrt{n}$ angegeben; also $H = h \cdot \sqrt{n}$. Für gerades m ist des weiteren (s.o.) $a = m^2 / 4$. Ausgehend von $N_{QR} = \left\lfloor \frac{1}{2a} \left(\sqrt{d + 4a \cdot H} - \sqrt{d - 4a \cdot H} \right) \right\rfloor$ hat man

$$N_{QR} = \left\lfloor \frac{2}{m^2} \left(\sqrt{d_e \cdot n + m^2 \cdot h \cdot \sqrt{n}} - \sqrt{d_e \cdot n - m^2 \cdot h \cdot \sqrt{n}} \right) \right\rfloor \qquad \textbf{(m gerade)}$$

Für $d_e \cdot n >> m^2 \cdot h \sqrt{n}$ – was in der Praxis immer gegeben sein wird – ergibt das (von Grenzfällen abgesehen) exakt: $N_{QR} = \left\lfloor \frac{2 \cdot h}{\sqrt{d_e}} \right\rfloor$. D.h. N_{QR} ist von m unabhängig.

Im Referenzfall (Basis-Version des QS) gilt: $N_{QR} = \left\lfloor \sqrt{n + h \cdot \sqrt{n}} - \sqrt{n - h \cdot \sqrt{n}} \right\rfloor$ und mit $n >> H$ hat man $N_{QR} = h$.

Unter Berücksichtigung, dass hier im Gegensatz zur Basisversion zwei Parabel-Äste zur Verfügung stehen, errechnet sich für $d_e < 16$ ein Vorteil; andererseits sollte d_e eine Grenze von 50 nicht überschreiten. D.h., dass ungerade Werte von m praktisch keine Verwendung finden können, falls $d_e > 12$ ist. Deshalb im weiteren m hier zur Vereinfachung der Darstellung immer als **gerade** angenommen.

Fazit: Die Eignung des Verfahrens hängt sehr davon ab, ob für $d_e < 50$ ein $n - d_e$ mit einer großen Zahl (möglichst kleiner) Primteiler existiert.

Wie viele Primteiler (einschließlich der Vielfachheiten) kleiner 10^5 die Zahl $n - d_e$ besitzt, kann mit Pollard's Rho-Verfahren für die infrage kommenden 12 Zahlen (da m als gerade vorausgesetzt, muss $n - d_e$ durch 4 teilbar sein) innerhalb weniger als 1 Sekunde festgestellt werden.
Wenn das Produkt Π der aufgefundenen kleinen Teiler durch 8 teilbar ist, ist die Anzahl der brauchbaren m-Werte mindestens gleich der Teileranzahl von Π (gleich Produkt der um 1 erhöhten Exponenten der Primteiler).
Die Teiler(-Paare) bis etwa 100 werden leicht durch Probedivision bestimmt, die weiteren Teilerpaare liefert das auf 4Π angewandte Fermat-Verfahren, wobei die gefundenen Teiler von 4Π jeweils durch 2 zu teilen sind.

Nun benötigt man zur Bestimmung der Koeffizienten b und c ($a = m^2 / 4$) außer m auch noch den Wert von e.
Zunächst wird für e = 0 eine Darstellung $d = d_0 \cdot n$ gesucht. Durch Einsetzen der Werte für g, v und r (s.o.) in die Definitionsgleichung $d = b^2 - 4ac$ ergibt sich – unter Benutzung der in Ziffer 3. erwähnten Zerlegung $(\frac{n-r}{m})^2 \bmod n = \frac{n(n \bmod m^2 - 2 \cdot r) + r^2}{m^2}$ – im **Fall I**.:

$$d_0 = m^2 - (n \bmod m^2 - 2 \cdot (n \bmod m)) \bmod m^2 .$$

Der Zusammenhang mit dem vorgegebenen d_e ist durch $d_e = d_0 - 2m \cdot e$ gegeben.; also $e = (d_0 - d_e) / 2m$. Das so errechnete e^* kann allerdings außerhalb der Grenzen $e_u = -(m - 2) \operatorname{div} 4 \le e \le m \operatorname{div} 4 = e_o$ liegen und ist – sofern dies zutrifft – durch ....

falls $e^* < e_u$: $e = e^* + m / 2$
falls $e^* > e_o$: $e = e^* - m / 2$ umzurechnen.

Fall II. läuft völlig analog, jedoch ist n durch $v \cdot n$ zu ersetzen:

$$d_0 = m^2 - (v \cdot (v \cdot n \bmod m^2 - 2 \cdot (v \cdot n \bmod m))) \bmod m^2 .$$

Außerdem ist in diesem Fall $e = (d_e - d_0) / 2m$.

<u>Zusammenfassende Darstellung des Verfahrens</u>
Gesucht: Koeffizienten a, b und c quadratischer Polynome mit gleicher Determinante d zu einer gegebenen Zahl n (> 10^{50} so dass die Begrenzung $m < n^{1/3}$ keine Rolle spielt)

1. **Bestimmung eines d_e, so dass $n - d_e$ möglichst viele Teiler < 10^5 besitzt.**
   - $f = n \bmod 8$
   - Untersuchung, welche der Zahlen $n - f - i \cdot 8$ ($i = 1, 2, .., 5$; $d_e = f + i \cdot 8$) die meisten kleinen Teiler besitzt. Für alle i:
     - Abdividieren der Teiler < 100; Exponenten abspeichern
     - Evtl. mit Rho-Verfahren weitere ungerade Teiler bestimmen (laufendes Abdividieren; Begrenzung der Iterationen auf z.B. 2000)
     - Je Zahl die Teiler-Anzahl (Produkt der je um 1 erhöhten Exponenten) sowie das Produkt der Teiler abspeichern
   - Auswahl der „besten" Zahl → d_e und Π (= Produkt der kleinen Teiler).
   - Auflisten und Abspeichern aller Teilerpaare von Π (z.B. mittels Faktorisierung von 4Π durch Fermat-Verfahren)

2. **Bestimmung geeigneter m-Werte und Berechnung von e**

a) Den jeweils nächsten (geraden) Teiler ‚m' ($> \sqrt{d_e}$) von Π auf Erfüllung eines der folgenden Kriterien untersuchen:

- Ist Π mod 2m = 0? Falls ja → Fall I. ; merken
- Ist m mod 8 = 4 ? Falls ja → Fall II.; merken
- Ist m mod 8 = 0 und Π mod 2m = m? Falls ja → Fall II.; merken

Kein Kriterium erfüllt; Gehe nach a) (nächster Teiler)
(Zu beachten: Für m = 2 steht nur ein Parabel-Ast (mit y < 0) zur Verfügung.
bei m = 4 stellen Fall I. und II. die selbe Parabel dar – also ist nur Fall I. auszuwerten.)

b) Bestimmung des zu m ‚gehörenden' e (in Form von Pseudo-Code):

```
If „Fall I." Then v = 1 Else  v = (m – 2) / 2
(*) g = (v*n) Mod m: If g > m / 2 And m Mod 4 <> 0 Then g = g – m
    x0 = (v*n – g) Div m
    r = (v*n) Mod m^2 – 2*g: If r < 0 Then r = r + m^2
    d0 = m^2 – (v*r) Mod m^2
    e = (de – d0)  Div (2*m): If v = 1 Then e = – e
    If e < – (m – 2) Div 4 Then e = e + m / 2
    If e >          m   Div 4 Then e = e – m / 2
```

3. **Berechnung der Koeffizienten usw.**

$a = m^2 / 4$ $b = m \cdot e - g$ $x_e = x_0 + e$ $c = x_e^2 \bmod n - n$ $d = b^2 - m^2 \cdot c = d_e \cdot n$

y-Werte an den 4 Intervallgrenzen: $\pm y_{\pm H} = \left\lfloor \frac{2}{m^2} (\sqrt{d \pm m^2 \cdot H}) \right\rfloor$

4. **Lösen der quadratischen (vorab) / linearen Kongruenzen mod p_i / Sieben**

Erstellen der Sieb-Matrix, Berechnen der QR, Auswerten: wie üblich
Falls nicht genügend QR über der Faktorbasis zerfallen: Wenn „Fall I." vorlag, prüfe, ob für dieses m auch „Fall II." gegeben ist (was häufig vorkommt). Wenn ja, setze v = (m – 2) / 2 und fahre mit (*) fort. Sonst gehe zu 2. und wähle das nächste m.

Anm.: Besonders günstig ist m mod 8 = 4; dann gibt es immer eine rechte und eine linke Parabel gleicher Diskriminante, und da **a** in beiden Fällen gleich ist, muss zur Lösung der lin. Kongruenz nur einmal invertiert werden. D.h. die Neujustierung des Siebes ist besonders einfach.

Fazit: Das Verfahren mit den „natürlichen" Polynomen funktioniert; ob es konkurrenzfähig ist, mag bei dem heutigen ausgefeilten Stand des QS zweifelhaft sein.
Interessant ist – neben den Einblicken in den inneren Aufbau des Systems der QR (die in der Darstellung zu kurz kamen) –, dass die Anzahl der auf dem beschriebenen Weg erhaltenen Parabeln mit vorgegebener Determinante $d_e \cdot n$ direkt von den Teilbarkeitseigenschaften der Zahl $n - d_e$ abhängt.

Anhang 1

I. Algorithmus zur Lösung der quadratischen Kongruenz $x^2 \equiv a \bmod p$

0. Prüfung, ob p eine Primzahl ist. Wenn nein, ist der Alg. nicht anwendbar.

1. Prüfung, ob a ein quadratischer Rest ist. Z.B. mittels Berechnung des Legendre-/Jacobi-Symbols $\left(\frac{a}{p}\right)$. Falls nein: Ausgabe „Keine Lösung möglich"; gehe nach 9. Sonst weiter mit 2.

2. Darstellung von $p - 1$ in der Form $2^k \cdot u$ mit ungerader Zahl u ==> k, u

3. Berechnung von $x = a^{\frac{u+1}{2}} \bmod p$
   Prüfung, ob $x^2 \bmod p = a$. Falls ja – z.B. wenn $p \equiv 3 \bmod 4$ – hat man eine Lösung gefunden; gehe nach 8. Sonst weiter mit Punkt 4.

4. Suche eines quadratischen Nicht-Restes m $\left(\frac{m}{p}\right) = -1$ ==> m

5. Berechne $c = m^u \bmod p$ und $b = a^u \bmod p$

6. Berechne die Ordnung von b: $\text{ord}_p[b] = 2^e$ ==> e (siehe unter (***)).

7. For j = 1 to k – 1
   $h = 2^{k-e-1}$ $f = c^h \bmod p$ $x = (f \cdot x) \bmod p$

   Prüfung, ob $x^2 \bmod p = a$. Falls ja, hat man eine Lösung gefunden; gehe nach 8. Sonst weiter mit nächster Zeile.

   $s = f^2 \bmod p$ $b = (s \cdot b) \bmod p$

   Berechne $\text{ord}_p[b] = 2^e$ ==> e
   Next j

8. Ausgabe der Lösung x
9. Ende

Hinweis: Es ist zweckmäßig , als Vertreter der Restklasse von a immer den kleinsten pos. Wert zu wählen; insbesondere die Prüfung, ob $x^2 \bmod p = a$ ist, gestaltet sich einfacher. Natürlich ändert sich dabei auch der Vertreter der Lösungs-Restklasse.

Nachstehend die Umsetzung der vorstehenden Schritte in ein Programm, das auch die Berechnung des Legendre-/ Jacobi-Symbols enthält.
Bei der Lösung der Kongruenz wird nach Restklassen (p mod 8) unterschieden, da der o.a. Algorithmus nicht nur im Fall p mod 4 = 3 sondern auch im Fall p mod 8 = 5 wesentlich abgekürzt werden kann.

Anm.: Der Alg. kann auch als Primzahl-Test dienen: Gibt der Alg. keine (korrekte) Lösung aus, ist der Modul mit Sicherheit keine Primzahl. Gilt auch die Umkehrung ?

Programm-Code zur Lösung von $x^2 \equiv a \bmod p$

Vorgabe: Primzahl p und a (Lösung genau dann, wenn a ist QR mod p ist)

```
'Schritt 1: Prüfen, ob a ein QR mod p ist; Jacobi-Symbol berechnen
   n=p      'Allgemein: n ungerade nat. Zahl; a ganze Zahl
   ar=a MOD n: b=n: js=1
   IF ar<0 THEN ar=ar+n
   ed=ar: ec=b: DO UNTIL ed=0: er=ec MOD ed: ec=ed: ed=er :LOOP: gg=ec
   IF gg>1 THEN PRINT "ggT(a,n)>1; d.h. SJ=0": EXIT
   DO WHILE ar>1
      DO WHILE ar MOD 4 =0
         ar=ar\4
      LOOP
      IF ar MOD 2 =0 THEN
         ar=ar\2
         IF b MOD 8=3 OR b MOD 8=5 THEN js=-js
      END IF
      c=b: b=ar: ar=c
      IF ar MOD 4=3 AND b MOD 4=3 THEN js=-js
      ar=ar MOD b
   LOOP
   PRINT "("a"/"n")","JS =";js
   IF js<>1 THEN PRINT "Keine Lösung vorhanden" :EXIT
'-----------------------------------------------
ar=a MOD p: IF ar<0 THEN ar=ar+p
p8=p MOD 8
PRINT "p MOD 8 =";p8

SELECT CASE p8 'Fallunterscheidung nach Restklassen mod 8
'=======================================================

       CASE 3,7  ' Berechnung von a^(p+1)/4 mod p
e=(p+1)/4: c=e: y=ar: IF c MOD 2=0 THEN x=1 ELSE x=y
DO WHILE c<>1
    c=c\2: y=(y*y) MOD p: IF c MOD 2=1 THEN x=(y*x) MOD p
LOOP
m=(x^2) MOD p
PRINT "("x"^2) mod"p"="m,ar
'=======================================================

       CASE 5
e=(p-1)/4: y=ar: c=e: IF c MOD 2=0 THEN x=1 ELSE x=y
DO WHILE c<>1
    c=c\2: y=(y*y) MOD p: IF c MOD 2=1 THEN x=(y*x) MOD p
LOOP             ' a^(p-1)/4 mod p = 1 oder -1
IF x=1 THEN
      e=(p+3)/8: y=ar: t=0
ELSE
      e=(p-5)/8: y=4*ar: x=x-p: t=1
END IF
c=e: IF c MOD 2=0 THEN x=1 ELSE x=y
DO WHILE c<>1
    c=c\2: y=(y*y) MOD p: IF c MOD 2=1 THEN x=(y*x) MOD p
LOOP
IF t=1 THEN x=(2*x*ar)MOD p
m=(x^2)MOD p
PRINT "("x"^2) mod"p"="m,ar
'=======================================================
```

```
       CASE 1 '(Löst auch die Fälle 3,5,7 mod 8)

'Schritt 2: Darstellung von p-1 als 2^k * u
u=p-1: k=0: par=0: DO WHILE par=0: u=u\2: par=u MOD 2: k=k+1: LOOP
PRINT u,k
' Schritt 3: Berechnung von a^(u+1)/2 mod p
x=ar: c=(u+1)/2: IF c MOD 2=0 THEN y=1 ELSE y=x
DO WHILE c<>1
    c=c\2: x=(x*x) MOD p: IF c MOD 2=1 THEN y=(x*y) MOD p
LOOP
x0=y: m=(x0^2)MOD p
IF m=ar THEN PRINT "H: ("x"^2) mod"p"="m,ar:EXIT

'Schritt 4: Suche nach einem quadratischem Nichtrest
d=1: js=1
DO UNTIL js=-1
   d=d+1: ed=d: ec=p
   DO UNTIL ed=0: er=ec MOD ed: ec=ed: ed=er :LOOP: gg=ec
   IF gg>1 THEN ITERATE
   r=d MOD p: b=p: js=1: IF r<0 THEN r=r+p
   DO WHILE r>1
      DO WHILE r MOD 4=0: r=r\4: LOOP
      IF r MOD 2 =0 THEN
         r=r\2: IF b MOD 8=3 OR b MOD 8=5 THEN js=-js
      END IF
      c=b: b=r: r=c: IF r MOD 4=3 AND b MOD 4=3 THEN js=-js
      r=r MOD b
   LOOP
LOOP
PRINT d;" ist QNR"

'Schritt 5: w = d^u mod p und b = a^u mod p berechnen
x=d: c=u: IF c MOD 2=0 THEN y=1 ELSE y=x
DO WHILE c<>1
    c=c\2: x=(x*x) MOD p: IF c MOD 2=1 THEN y=(x*y) MOD p
LOOP
        w=y
x=ar: c=u: IF c MOD 2=0 THEN y=1 ELSE y=x
DO WHILE c<>1
    c=c\2: x=(x*x) MOD p: IF c MOD 2=1 THEN y=(x*y) MOD p
LOOP
        b=y

'Schritt 6: Ordnung von b in Z_p^* bestimmen
bi=b: e0=0
DO WHILE bi<>1: e0=e0+1: bi=(bi*bi)MOD p: LOOP
PRINT "ORD b:";e0
'Schritt 7: Lösung suchen und finden
FOR j=0 TO k
    x=w: c=2^(k-e0-1): IF c MOD 2=0 THEN y=1 ELSE y=x
    DO WHILE c<>1
        c=c\2: x=(x*x) MOD p: IF c MOD 2=1 THEN y=(x*y) MOD p
    LOOP
    f=y
    x0=(f*x0)MOD p: m=(x0^2)MOD p
    IF m=ar THEN EXIT FOR
    s=(f^2)MOD p: b=(s*b)MOD p
    bi=b: e0=0
    DO WHILE bi<>1: e0=e0+1: bi=(bi*bi)MOD p: LOOP
NEXT j
PRINT "W: ("x0"^2) mod"p"="m,ar
END SELECT
```

II: Lösen der quadratischen Kongruenz $x^2 \equiv a \bmod n$ (n zusammengesetzt)

Zunächst ist zu prüfen, ob a ein QR zu allen Primfaktoren von n ist, da es nur dann Lösungen gibt.

Sei $n = 2^{\alpha} \cdot u$ mit $u = \prod_{\beta_i > 0} p_i^{\beta_i}$ mit $p_i > 2$

1. Ist ggT(a, n) > 1 → a ist kein QR zum Modul n; sonst weiter mit 2.

2. $\alpha < 2$: → weiter mit 3.
   $\alpha = 2$: Ist a mod $4 \neq 1$ → a ist kein QR; sonst weiter mit 3.
   $\alpha > 2$: Ist a mod $8 \neq 1$ → a ist kein QR; sonst weiter mit 3.

3. Für alle p_i aus u ist $\left(\frac{a}{p_i}\right)$ zu bestimmen

   Ist für <u>alle</u> p_i das Legendre-Symbol gleich 1 → a ist QR; sonst: a ist QNR
   (Ist $n = 2^{\alpha}$ – also u = 1 – entfällt Schritt 3. natürlich.)

<u>Beispiel 1</u>:

Seien $n = 2 \cdot 1987^2 = 7896338$ (1987 ist prim) und a = 8123 → a mod 1987 = 175
Die Berechnung des Legendre-/Jacobi-Symbols ergibt $\left(\frac{175}{1987}\right) = 1$. Also ist 8123 QR zum Modul n; d.h. $x^2 \equiv 8123 \bmod 7896338$ besitzt Lösungen.

Probe: Für $x_1 = 3105913$ und $x_2 = n - x_1 = 4790425$ gilt
$x_1^2 = 3105913^2 \equiv 8123 \bmod 7896338$ und $x_2^2 = (n - x_1)^2 \equiv 8123 \bmod 7896338$.

<u>Beispiel 2</u>:

$n = 2^2 \cdot 3^3 \cdot 17 = 1836$ Ist a = 1021 ein QR zu diesem Modul?
Dazu muss 1021 mod 4 = 1 sein und QR zu den Moduln 3 und 17

$1021 \equiv 1 \bmod 4$ → Bedingung erfüllt

$1021 \equiv 1 \bmod 3$; 1 ist QR mod 3; alternativ: Berechnung von $\left(\frac{1021}{3^3}\right) = 1$ (hier muss nicht auf p = 3 reduziert werden, da der Exponent von 3 ungerade ist) → Bedingung erfüllt

$\left(\frac{1021}{17}\right) = 1$ → Bedingung erfüllt

1021 ist also ein QR zum Modul 1836; d.h. $x^2 \equiv 1021 \bmod 1836$ besitzt Lösungen.

Die 4 Lösungspaare sind:

x_1	$x_2 = n - x_1$
101	1735
169	1667
749	1087
817	1019

Wie man diese Lösungen findet, wird im Beispiel 4 erläutert.

Dagegen ist 1021 kein QR zum Modul $8 \cdot 3^3 \cdot 17$, da 1021 mod 8 = 5 ≠ 1.
In der Tat findet man kein x, das die Kongruenz $x^2 \equiv 1021 \bmod 3672$ erfüllt.

Beispiel 3: Alle Lösungen von $x^2 \equiv 7 \bmod 1457$; $1457 = 31 \cdot 47$; 7 ist QR mod 31 u. 47

Mit dem o.a. Tonelli-Alg. erhält man:

$x^2 \equiv 7 \bmod 31 \implies x = \pm 10$ $\qquad$ $x^2 \equiv 7 \bmod 47 \implies x = \pm 17$

Anwendung des Chin. Restsatzes auf die vier Lösungspaare:

$\left.\begin{array}{l} x \equiv 10 \bmod 31 \\ x \equiv 17 \bmod 47 \end{array}\right\}$ $x_1 \equiv 816 \bmod 1457$ $\qquad$ $\left.\begin{array}{l} x \equiv 10 \bmod 31 \\ x \equiv -17 \bmod 47 \end{array}\right\}$ $x_2 \equiv 1064 \bmod 1457$

$\left.\begin{array}{l} x \equiv -10 \bmod 31 \\ x \equiv -17 \bmod 47 \end{array}\right\}$ $x_3 \equiv 641 \bmod 1457$ $\qquad$ $\left.\begin{array}{l} x \equiv -10 \bmod 31 \\ x \equiv 17 \bmod 47 \end{array}\right\}$ $x_4 \equiv 393 \bmod 1457$

Zum Chinesischen Restsatz siehe **Abschnitt IV im Anhang 2**

Beispiel 4: (Berechnung der Lösungen zu Beispiel 2)

Wie in Beispiel 2 gezeigt, ist die Kongruenz $x^2 \equiv 1021 \bmod 4 \cdot 3^3 \cdot 17$ (= 1836) lösbar. Um die Lösungen konkret zu finden, sind zunächst die Lösungen zu den drei Faktoren 4, 3, 17 des Modul zu bestimmen:
Diese sind wegen
$x^2 \equiv 1021 \bmod 4 \equiv 1 \bmod 4$; $x^2 \equiv 1021 \bmod 3 \equiv 1 \bmod 3$; $x^2 \equiv 1021 \bmod 17 \equiv 1 \bmod 17$
in allen drei Fällen (zufällig) $x_{1,2} = \pm 1$ zum betr. Modul.
(Wenn die Dinge nicht so einfach liegen, ist der Tonelli-Alg. zu bemühen.)
Nun sind die Lösungen zum Modul 3 auf den Modul 3^3 anzuheben, wie das in Abschnitt II. des Anhang 2 beschrieben ist. Da das Polynom die einfache Form $f(x) = x^2 - a$ $(f'(x) = 2x)$ besitzt, genau zwei Lösungen für jeden Modul p^k $(k = 1, 2, 3)$ existieren (a ist QR) und diese von Null verschieden sind, geht das besonders einfach:

> Sei x_1 eine Lösung zu $x^2 \equiv a \bmod p^k$.
> Mit $B = (x_1^2 - a) \bmod p^{k+1}$ und $s = [\frac{-B}{p^k} \cdot (2x_1)^{p-2}] \bmod p$ ist dann
> $y_1 = x_1 + s \cdot p^k$ eine Lösung zum Modul p^{k+1}

Beginnend mit k =1 und $x_1 = 1$ erhält man durch rekursive Anwendung (setze $x_1 = y_1$ und $k = k + 1$) folgende Werte: $x_1 = 2$ zu 3^2 und $x_1 = 7$ zu 3^3. (Die zweite Lösung x_2 ist jeweils $p^{k+1} - x_1 = -x_1$).

Alle Lösungen von $x^2 \equiv 1021 \bmod 4 \cdot 3^3 \cdot 17$ ergeben sich wiederum (siehe Beispiel 3) durch Lösen aller simultanen Kongruenzen, die durch Kombinieren der jeweils zwei Lösungen zu den drei Moduln 4, 27, 17 (also 2^3 Möglichkeiten) gebildet werden können:

$x \equiv x_{1,2} \bmod 4 \rightarrow$	1	1	1	1	–1	–1	–1	–1
$x \equiv x_{1,2} \bmod 27 \rightarrow$	7	7	–7	–7	7	7	–7	–7
$x \equiv x_{1,2} \bmod 17 \rightarrow$	1	–1	1	–1	1	–1	1	–1
Lösungen $x_1,..,x_8$:	817	169	749	101	1735	1087	1667	1019

Wie man sieht, reicht es (bei geeigneter Auswahl) aus, nur 4 simultane Kongruenz-Systeme zu lösen, da die weiteren 4 genau die komplementären Lösungen ($x_1 + x_2 = n$) darstellen. Das ist der Fall, wenn die drei $x_{1,2}$ –Werte je mit –1 multipliziert werden.

Anhang 2

I. Allgemeine quadratische Kongruenz $f(x) = a \cdot x^2 + b \cdot x + c \equiv 0 \bmod m$ lösen

(a, b, c: ganze Zahlen; $a \neq 0$ (sonst lin. Kongruenz); $c \neq 0$)

Eine quadratische Kongruenz der obigen Form zu einem Modul $m = \prod {p_i}^{\alpha_i}$ ist lösbar, wenn es zu jedem ${p_i}^{\alpha_i}$ Lösungen gibt. Lösungen zu ${p_i}^{\alpha_i}$ existieren wiederum nur, wenn es Lösungen zum Modul p_i gibt. (Dabei sind natürlich auch etwaige triviale Lösungen in die Lösungsmenge einzubeziehen.)

Falls für einen Modul p_i gilt: $p_i \mid a$ (also $a \bmod p_i = 0$), sind hinsichtlich der verbleibenden linearen Kongruenz modulo p_i drei Fälle zu unterscheiden:

(α): $b \neq 0 \bmod p$	Einzige Lösung folgt aus $b \cdot x \equiv -c \bmod p$
(β): $b \equiv c \equiv 0 \bmod p$ („Nullpolynom“)	Alle p Restklassen sind Lösungen
(γ): $b \equiv 0 \bmod p$ und $c \neq 0 \bmod p$	Keine Lösung

Damit ist der Fall $p_i \mid a$ erledigt und kann für das Weitere ausgeschlossen werden.

1. m enthält den Primfaktor p = 2

Ob zum Modul 2 Lösungen existieren, kann nach Reduktion der Koeffizienten mod 2 leicht „von Hand“ überprüft werden, da – abgesehen von dem oben abgearbeiteten Fall $p_i \mid a$ – nur die (auf das kleinste pos. Restesystem reduzierten) Gleichungen $x^2 + x \equiv 0 \bmod 2$ bzw. $x^2 + 1 \equiv 0 \bmod 2$ sowie $x^2 \equiv 0 \bmod 2$ mit den Lösungen: $x_0 = 0, 1$ bzw. $x_0 = 1$ bzw. $x_0 = 0$ zu betrachten sind.
(Am zweckmäßigsten wird es beim Modul 2 immer sein, f (x) für die Werte 0 und 1 ‚durchzuprobieren’; dann erübrigen sich alle Fallunterscheidungen.)

2. ungerade Primfaktoren p von m

Maßgeblich für die Anzahl der Lösungen von $f(x) \equiv 0 \bmod p$ ($p > 2$) ist der Wert des Legendre-Symbols $\left(\frac{D}{p}\right)$ mit $D = b^2 - 4ac$.

$$\left(\frac{D}{p}\right) = \begin{cases} 1: & f(x) \equiv 0 \bmod p \text{ besitzt 2 inkongruente Lösungen} \\ 0: & p \mid D;\ \text{die einzige Lösung folgt aus } 2ax \equiv -b \bmod p \\ -1: & \text{es gibt keine Lösung } x_0 \text{ mit } f(x_0) \equiv 0 \bmod p \end{cases}$$

Ist $\left(\frac{D}{p}\right) = 1$, erhält man die beiden Lösungsrestklassen in zwei Schritten:

a): **Quadratische Kongruenz $(2ax + b)^2 \equiv D \bmod p$ lösen**

Ist ggT (k, p) = 1 hat die quadratische Kongruenz $k \cdot f(x) \equiv 0 \bmod p$ die gleichen Nullstellen wie $f(x) \equiv 0 \bmod p$. Dies nutzt man – im Fall ungerader Primzahl-Moduln – zur äquivalenten Umformung der ursprünglichen Kongruenz mittels quadratischer Ergänzung: $4a \cdot f(x) \equiv (2ax + b)^2 - (b^2 - 4ac) \equiv 0 \bmod p$, d.h. die allgemeine quadr. Kongruenz wird in die Normalform $y^2 \equiv D \bmod p$ gebracht und ist somit dem im Anhang 1 beschriebenen Verfahren zugänglich, das die beiden Lösungen y_1 und y_2 ($= -y_1$) liefern möge.

b): L**ineare Kongruenz $2ax + b \equiv \pm y_1 \bmod p$ lösen**

Für jedes Vorzeichen hat die betr. Kongruenz (wegen ggT(2a, p) = 1) genau eine Lösung. Zusammengefasst lauten diese:

$$x_{1,2} \equiv (\pm y_1 - b)\cdot(2a)^{p-2} \bmod p$$

(Die Auflösung nach x ermöglicht der Satz von Euler: $e^{\varphi(n)} \equiv 1 \bmod n$ falls ggT(e, n) = 1. Hier ist φ(n) = p – 1 und die Multiplikation der Kongruenz mit $(2a)^{p-2}$ ergibt wegen $(2a)\cdot(2a)^{p-2} \equiv 1 \bmod p$ sofort die vorstehende Lösungsformel.)

Zur Ausrechnung des Terms $(2a)^{p-2}$ siehe <u>Anhang 1</u> unter (**).

(Häufig wird auch der Erweiterte Euklidische Algorithmus zur Lösung linearer Kongruenzen verwendet; siehe dazu nachstehende Ergänzung 1)

Hat man nun zu allen in der Primfaktor-Zerlegung von m vorkommenden p_i (alle) Lösungen gefunden, gilt es diese noch für die entsprechenden Primzahl-Potenzen zu bestimmen. Das kann mittels des sog. Hensel-Lifting, welches im folgenden Punkt beschrieben wird, geschehen.
Wenn das alles erledigt ist, können mit Hilfe des Chinesischen Restsatzes schlussendlich die gesuchten Lösungen zum Modul m angegeben werden.
Anzahl der Lösungen: Zu den k Primfaktoren p_i von m gebe es je t_i Lösungen; dann beträgt die Anzahl der Lösungen zum Modul m insgesamt $\prod_{1}^{k} t_i$.

Ergänzung 1: Lineare Kongruenz mit erweitertem Euklidischen Algorithmus (EEA) lösen

Gesucht sind die Lösungen x_i der Kongruenz $A\cdot x \equiv B \bmod M$
Es sei d = ggT (A, M)
Falls gilt: d teilt B nicht → die Kongruenz besitzt <u>keine</u> Lösung.
Anderenfalls existieren d Lösungen $x_t = x_0 + t\cdot M / d$, wobei t alle Werte zwischen 0 und d – 1 durchläuft.
Die „Grundlösung“ x_0 soll nun mit dem EEA bestimmt werden.
Es sei a = A / d, b = B / d und m = M / d und somit ggT (a, m) = 1.
(Keineswegs erforderlich, aber übersichtlicher ist es, a und b als kleinste positive Reste darzustellen → a = a mod m: if a < 0 then a = a + m; b analog.)

<u>Algorithmus EEA</u>

```
e = a:  c = m: u1 = 1: u2 = 0: v1 = 0: v2 = 1
Do while c <> 0
        q = e div c:  r = e mod c
        u3 = u1 – q * u2:  v3 = v1 – q * v2
        e = c: c = r:  u1 = u2:  v1 = v2:  u2 = u3:  v2 = v3
Loop
x0 = (u1 * b) mod m
```

(Die Anwendung des EEA zur Lösung linearer Kongruenzen mit ggT (a, m) = 1 beruht auf der Äquivalenz zur Lösung der diophantischen Gleichung a·x + b·y = 1)

II. Polynomkongruenzen modulo einer Primzahlpotenz lösen

Gegeben sei ein Polynom f(x) mit ganzzahligen Koeffizienten und x_0 sei eine Lösungsrestklasse zum Modul p^k; also $f(x_0) \equiv 0 \bmod p^k$
Gesucht ist eine Lösung der Kongruenz $f(x) \equiv 0 \bmod p^{k+1}$
Eine solche Lösung – wenn sie denn existiert – lässt sich rekursiv mittels des sog. Hensel-Lifting finden (nachfolgend für diese spezielle Anwendung im Sinne eines „Kochrezeptes" beschrieben).

1. **Schritt:** Ausrechnung der Ableitung $A = f'(x_0) \bmod p$ sowie von $B = f(x_0) \bmod p^{k+1}$

   (Die Koeffizienten von $f'(x)$ können von vornherein ‚mod p' reduziert werden; die von f(x) sind – falls erforderlich – für jeden Wert von k erneut zu reduzieren, da der Modul immer größere Werte annimmt.)

2. **Schritt:** Fallunterscheidung. Es sind drei Fälle zu unterscheiden:
   a) <u>$A \neq 0$</u>
   Es gibt genau ein s, so dass $f(x_0 + s \cdot p^k) \equiv 0 \bmod p^{k+1}$
   Dieses s erhält man durch Lösen der lin. Kongruenz
   $A \cdot s \equiv C \bmod p$ mit $C = -B / p^k$
   → $s_1 = C \cdot A^{p-2} \bmod p$; Lösung: $e = x_0 + s_1 \cdot p^k$
   Gehe zu 3. (Falls $p = 2$, ist $s_1 = |C| \bmod 2$)

   b) <u>$A = 0$ und $B = 0$</u>
   Für alle s mit $0 \leq s \leq p - 1$ ist $f(x_0 + s \cdot p^k) \equiv 0 \bmod p^{k+1}$
   Wähle eine beliebige Lösung $e = x_0 + s \cdot p^k$ aus und gehe zu 3.
   (Evtl. ist jede einzelne Lösung zu befragen, ob sie sich liften lässt.)

   c) <u>$A = 0$ und $B \neq 0$</u>
   Es gibt **auf Basis der Lösung x_0 mod p^k** kein x, so dass $f(x) \equiv 0 \bmod p^{k+1}$
   Gehe zu 1. und wähle anderes x_0 (falls existent); sonst: Ende des Verfahrens.

3. **Schritt:** Setze $x_0 = e$ und $k = k + 1$; weiter mit Schritt 1., (falls noch höhere Potenzen untersucht werden sollen.)

<u>Hinweis:</u> 1.Ist die höchste Potenz von x in f(x) größer 2, so sind keine allgemeinen Verfahren zur Ermittlung einer Lösung mod p bekannt. In diesen Fällen bleibt also nur, die Ausgangslösung zum Starten des Hensel-Lifting mittels Probieren zu finden.
Für kleine Moduln p ist das auch für die höheren Potenzen des Modul die einfachere Methode.

2. Gibt es zum Modul p^k mehrere Lösungen, so ist die Prozedur ggf. für alle Lösungen durchzuführen, da u.U. nicht jedes x_0 eine Lösung mod p^{k+1} nach sich zieht (was nachstehend auch an Beispielen (Nr. 4. und 5.) gezeigt wird).

Beispiele: (in großer Zahl, um die „Unberechenbarkeit“ zu veranschaulichen)

1. $f(x) = x^4 - 3x^3 + 27$ $\quad p = 13$ $\quad f'(x) = 4x^3 - 9x^2$

k	Nullstellen	Fall / Kommentar
1	8, 4	durch Probieren
2	47, 56	Fall 1; und zwar hat jede Nullstelle mod p^k
3	554, 732	genau eine „Nachfolgerin“ mod p^{k+1}
usw.		

2. $f(x) = x^4 - 3x^3 + 27$ $\quad p = 3$ $\quad f'(x) = x^3$ (reduziert)

k	Nullstellen	Fall / Kommentar
1	0	
2	0, 3, 6	Für k = 2 (Fall 2) folgt für jede der
3	0, 3, 6, 9, 12, 15, 18, 21, 24	3 Nullstellen wiederum Fall 2, so dass
4	keine	es für k = 3 sogar 9 Nullstellen gibt. Keine hat für k = 4 einen Nachfolger (Fall 3).

3. $f(x) = x^4 - 3x^3 - x^2 + 12$ $\quad p = 7$ $\quad f'(x) = 4x^3 - 9x^2 - 2x$

k	Nullstellen	Fall / Kommentar
1	2	
2	2	Fall 1 mit immer gleicher Lösungsrestklasse
3	2	
usw.		

4. $f(x) = x^3 - 2x^2 + 5x + 1$ $\quad p = 5$ $\quad f'(x) = 3x^2 - 4x + 5$

k	Nullstellen	Fall / Kommentar
1	1, 3	
2	6, 3, 8, 13, 18, 23	Die „1“ hat Fall 1 zur Folge → 6 → 56 usw.
3	56	Die „3“ hat Fall 2 mit 5 Lösungen zur Folge, von denen
4	306	sich keine weiter liften lässt (Fall 3).
usw.		

5. $f(x) = x^4 - 2x^3 + 5x + 2$ $\quad p = 5$ $\quad f'(x) = -x^3 - x^2$ (red.)

k	Nullstellen	Fall / Kommentar
1	4	Für k = 2 liegt Fall 2 vor. Von den 5 Lösungen
2	4, 9, 14, 19, 24	lassen sich nur 2 (14 und 24) weiter liften und zwar
3	14, 24, 39, 49, 64, 74, 89, 99, 114, 124	ebenfalls unter Fall 2. Das setzt sich so weiter fort.
4	usw.: stets 10 Lösungen	

Schließlich noch 4 Beispiele zum Modul 2^k

$f(x) = x^2 - 5$

$2 \rightarrow 1$
$4 \rightarrow 1, 3$ Fall 2
$8 \rightarrow$ keine Lösung,
da 5 kein QR mod 2^3

$f(x) = x^2 - 33$

$2 \rightarrow 1$
$4 \rightarrow 1, 3$ Fall 2
$8 \rightarrow 1, 3, 5, 7$
$16 \rightarrow 1, 7, 9, 15$ Für alle weiteren 2^k gibt es 4 Lösungen, da $33 \equiv 1 \bmod 8$

$f(x) = -3x^5 + 6x^2 - 33$

$2 \rightarrow 1$
$4 \rightarrow 3$
$8 \rightarrow 7$
$2^4 \rightarrow 7$
$2^5 \rightarrow 23$
usw.

$f(x) = -3x^2 + 6x - 7$

$2 \rightarrow 1$
$4 \rightarrow 1, 3$
$8 \rightarrow 3, 7$
$2^4 \rightarrow 3, 7, 11, 15$
$2^5 \rightarrow$ keine Lösung

III. Ausführliche Beispiele zur Lösung quadratischer Kongruenzen:

Es sei **$f(x) = -191 \cdot x^2 + 614 \cdot x - 244$** **$m = 73$**

Gesucht: Die Lösungsrestklassen für $f(x) \equiv 0 \bmod 73$ (73 ist Primzahl)

Reduktion der Koeffizienten mod 73 : $-45 \cdot x^2 + 30 \cdot x - 25 \equiv 0 \bmod 73$

Diskriminante: $30^2 - 4 \cdot (-45) \cdot (-25) = -3600 \rightarrow D \bmod 73 = -23$
Berechnung Legendre-Symbol: $\left(\frac{D}{p}\right) = \left(\frac{-23}{73}\right) = 1 \rightarrow$ Es gibt Lösungen.
Berechnung der Lösungen:

1. Schritt: $y^2 \equiv -23 \bmod 73$ lösen
   Der Tonelli-Alg. erbringt $y_{1,2} = \pm 14$

2. Schritt: x-Werte aus $(2 \cdot (-45) \cdot x + 30 \equiv \pm 14 \bmod 73$ bestimmen
   Lösung mit obiger Formel: $x_{1,2} \equiv (\pm 14 - 30) \cdot (-90)^{71} \bmod 73 \rightarrow x_1 = 31; x_2 = 67$

Probe: Die Werte von $f(x_1)$ und $f(x_2)$ sind ohne Rest durch 73 teilbar.

$f(x) = 171 \cdot x^2 + 2220 \cdot x + 8364$ **$m = 2^3 \cdot 3^2 \cdot 5^3 = 9000$**

Modul $2 \rightarrow$ red.: $x^2 \equiv 0 \rightarrow x_0 = 0$
Modul $3 \rightarrow$ red.: $0 \equiv 0 \rightarrow x_0 = \{0, 1, 2\}$
Modul $5 \rightarrow$ red.: $x^2 \equiv -4 \rightarrow D = 0^2 - 4 \cdot 1 \cdot 4 = -16 \rightarrow \left(\frac{-16}{5}\right) = 1 \rightarrow$ Tonelli: $x_0 = \{1, 4\}^{*)}$

*): Das Ergebnis $x_0 = \pm 1$ von $x^2 \equiv 1 \bmod 5$ kann man durchaus auch ohne Rechner-Unterstützung finden.

Fazit: Es existieren zu allen Primfaktoren der Zerlegung von m Lösungen, so dass nun die Primzahl-Potenzen untersucht werden können (Hensel-Lifting).

	mod 2	mod 2^2	mod 2^3
Modul 2^3:	$x_0 = 0 \rightarrow$	0 $\rightarrow$	keine Lösung (Fall 3)
		2 $\rightarrow$	Lösungen: **2, 6**

	mod 3	mod 3^2
Modul 3^2:	$x_0 = 0 \rightarrow$	keine Lösung
	$x_0 = 1 \rightarrow$	Lösungen: **1, 4, 7**
	$x_0 = 2 \rightarrow$	keine Lösung

	mod 5	mod 5^2	mod 5^3
Modul 5^3:	$x_0 = 1 \rightarrow$	11 $\rightarrow$	Lösung: **86**
	$x_0 = 4 \rightarrow$	19 $\rightarrow$	Lösung: **94**

Aus den sieben vorstehend ermittelten Werten, können 12 verschiedene Tripel gebildet werden, aus denen per Restsatz jeweils eine Lösung modulo m resultiert:

z.B.: $x \equiv 6 \bmod 8$
$x \equiv 7 \bmod 9$
$x \equiv 86 \bmod 125$
} $x \equiv 2086 \bmod 9000$

Alle Ergebnisse in Tabellenform:

Modul:8	9	125	9000	8	9	125	9000
2	1	86	**586**	6	1	86	**5086**
2	1	94	**1594**	6	1	94	**6094**
2	4	86	**3586**	6	4	86	**8086**
2	4	94	**4594**	6	4	94	**94**
2	7	86	**6586**	6	7	86	**2086**
2	7	94	**7594**	6	7	94	**3094**

Zum Umgang mit linearen Kongruenz-Systemen, zu denen eine simultane Lösung gesucht ist, siehe folgenden **Abschnitt IV**.

IV. System linearer Kongruenzen lösen

Der **Chinesische Restsatz** besagt (unter anderem), dass es zu einem System von k linearen Kongruenzen $x \equiv c_i \bmod m_i$ genau dann eine Restklasse x zum Modul M gibt, die alle k Kongruenzen simultan erfüllt, wenn folgende Voraussetzung erfüllt ist:

Für alle $1 \le i, j \le k$ mit $i \ne j$ gilt: $ggT(m_i, m_j) \mid (c_i - c_j)$.

Es ist $M = kgV(m_1,...m_i,...m_k)$

(Im ‚Regelfall' sind alle m_i paarweise teilerfremd und somit $M = m_1 \cdot\cdot m_i \cdot\cdot m_k$)

Es folgen einige Hinweise, wie die Bearbeitung eines ‚allgemeinen' linearen Kongruenzsystems per Rechner zweckmäßigerweise angegangen werden kann.
(Sind alle m_i Primzahlen, geht es auch wesentlich einfacher.)

Schritt 0 (Eingabe / Umformung)

Definiere einen zweidimensionalen Bereich (Matrix) f (i, j) mit $i \le k$ und $j \le 8$
Eingabe der lin. Kongr. in der Form $a_i \cdot x \equiv b_i \bmod m_i$:
$f(i, 1) = a_i$, $f(i, 2) = b_i$, $f(i, 3) = m_i$ ((Meist ist $a_i = 1$))
Bringe alle Kongruenzen in die Form $x \equiv c_i \bmod m_i$ und setze $f(i, 4) = c_i$. D.h., falls $a_i \ne 1$, berechne $c_i = a_i^{-1} \cdot b_i \bmod m_i$, sonst $c_i = b_i$. ($a^{-1} \equiv a^{\varphi(m)-1} \bmod m$; besser mit EEA)
Existiert a_i^{-1} in einem Fall nicht → „Kongr.-System ist nicht lösbar" → Ende

Setze $f(i, 5) = m_i$ ((So bleiben die ursprünglichen Eingaben in f (i, 1) bis f (i, 3) erhalten und können erf. auf Fehler kontrolliert werden.))
Wandle alle c_i in kleinste pos. Reste um: (nicht nötig, aber zweckmäßig)

```
For i = 1 to k
    f (i, 4) = f (i, 4) mod f (i, 5)
    Ist f (i, 4) < 0 → f (i, 4) = f (i, 4) + f (i, 5)
Next i
```

Schritt 1 (Prüfen der Lösbarkeit)

```
For i = 1 to k – 1
    For j = i + 1 to k
    Berechne d = ggT (mi, mj); Prüfung, ob (ci – cj) mod d = 0 ? Falls nein →
     „Wegen i-ter und j-ter Kongruenz keine Lösung vorhanden" → Ende.
    Next j
Next i
```

Schritt 2 (Sukzessives Lösen)

Es wird jeweils die Lösung der i*-ten und der i + 1-ten Kongruenz berechnet, wobei die i*-te selbst das Ergebnis vorangegangener „Zusammenfassungen" ist.
Setze f (1, 6) = f (1, 4); f (1, 7) = f (1, 5) ((1*-te Kongr. = 1-te Kongr. ist Startwert))

```
For i = 1 to k – 1
    Berechne Lösung c*i+1 der Kongruenzen
        i*   :  c1 = f (i, 6);      m1 = f (i, 7)   und
        i +1 :  c2 = f (i +1, 4);   m2 = f (i +1, 5)  mit Alg. CR (s.u.)
    Ergebnis CR: f (i +1, 6) = c; f (i +1, 7) = m
    Laufende Prüfung (kann sinnvoll sein)
    For j = 1 to i +1
    r = f (i +1, 6) mod f (j, 3)
    Wenn  r ≠ f (j, 4) → „Fehler in der i +1-ten Kongruenz"→ Ende
    Next j
Next i
```

Schritt 3 (Endergebnis)

„Die Restklasse" f (k, 6) „zum Modul" f (k, 7) „erfüllt alle Kongruenzen simultan"

Algorithmus CR (Berechnet Lösung zweier simultaner Kongruenzen)

Gegeben:	Gesucht:
$x \equiv c1 \bmod m1$	$x \equiv c \bmod m$ wobei gilt:
$x \equiv c2 \bmod m2$	$c \equiv c1 \bmod m1$ und $c \equiv c2 \bmod m2$

Lösung mittels EEA [Darstellung ggT (m1, m2) = u·m1 + v·m2)]

```
d = m1: e = m2: u1 = 1: v1 = 0: u2 = 0: v2 = 1
Do while e<>0
        q = d div e: r = d mod e: u3 = u1– q*u2: v3 = v1– q*v2
        d = e: e = r: u1 = u2: v1 = v2: u2 = u3: v2 = v3
Loop
If  (c1 – c2) mod d <> 0  then
         " Kongruenzsystem nicht lösbar "
else
         s = (c1 – c2) div d: m = (m1* m2) div d: c = (c1 – u1* m1*s) mod m
         If c < 0 then c = c + m
         "Die Restklasse  c zum Modul m erfüllt die beiden Kongruenzen"
End if
```

Durch sukzessives Lösen (Zusammenfassung) je zweier Kongruenzen ist so jedes Kongruenzsystem lösbar (, wenn Lösungen existieren).