

Numerische Auflösung quadratischer Congruenzen für jeden einfachen Modul.

Die im Vorangehenden dargestellte Methode lässt sich mit einigen Modificationen auch zur Lösung quadratischer Congruenzen benützen.

Ist in der Congruenz $y^2 \equiv d \pmod{b}$ der Modul b eine einfache und d eine unter ihm liegende positive oder negative Zahl, so untersuche man zunächst, ob $+b$ oder $-b$ ein quadratischer Rest von d ist. Im bejahenden Falle hat man die, jene Congruenz vertretende Gleichung $y^2 = bx + d$ auf die unter (II) im vorigen Abschnitte vorgeschriebene Form zu bringen; im verneinenden, zumeist vorkommenden Falle hingegen, bilde man aus d durch successives Hinzuaddiren von $+b$ wie auch nebenbei von $-b$ eine solche kleinste Zahl $c = d \pm nb$, dass $+b$ oder $-b$ ein quadratischer Rest von c , und dabei der grösste Divisor von c kleiner als b werde; doch dürfen diese Zahlen nicht beide zugleich negativ sein, weil sonst die spätere Gleichung [4] unmöglich wäre. Hierauf gebe man der mit der Congruenz $y^2 \equiv c \pmod{b}$ äquivalenten Gleichung

$$y^2 = bx + c \quad [1]$$

die Form

$$y^2 = (\alpha x + \beta)^2 - (\gamma x + \delta)(\epsilon x + \zeta), \quad [2]$$

was dadurch bewerkstelligt wird, dass man zu [1] die identische Gleichung $0 = (\alpha x + \beta)^2 - \alpha^2 x^2 - 2\alpha\beta x - \beta^2$ hinzuaddirt, in welcher α und β noch unbestimmte Zahlen bezeichnen.

Damit in der so erhaltenen Gleichung

$$y^2 = (\alpha x + \beta)^2 - [\alpha^2 x^2 + (2\alpha\beta - b)x + (\beta^2 - c)]$$

das eckig eingeklammerte Trinom ein Product zweier linearen Factoren werde, muss seine Determinante ein Quadrat sein; also

$$(2\alpha\beta - b)^2 - 4\alpha^2(\beta^2 - c) = \Delta^2 \text{ oder } \Delta^2 = 4c\alpha^2 - 4b\alpha\beta + b^2;$$

setzt man hier $\Delta = 2p\alpha + b$, so wird $\alpha = -\frac{b(p+\beta)}{p^2-c}$ und für $p = \frac{v}{w}$:

$$\alpha = -\frac{bw(v+\beta w)}{v^2-cw^2} \quad [3]$$

Bestimmt man aus der, wegen der oben herbeigeführten Beschaffenheit von b und c , in Rationalzahlen möglichen Gleichung

$$v^2 - cw^2 = \pm b \quad [4]$$

die Grössen v und w nach der im ersten Abschnitte angegebenen Methode, und setzt die gefundenen positiv zu nehmenden Werthe v_0 und w_0 in die Gleichung [3] ein, so wird

$$\alpha = \mp w_0(v_0 + w_0\beta) \quad [5]$$

Nun ist der Unbestimmten β ein solcher Werth zu ertheilen, dass α eine möglichst kleine ganze Zahl werde, was bei einem ganzzahligen w_0 sogleich erreicht wird, wenn man für β die dem Quotienten $-\frac{v_0}{w_0}$ nächst liegende negative ganze Zahl setzt, sonst aber durch Lösung einer unbestimmten einfachen Gleichung zu Stande kömmt. Ist nämlich $w = \frac{\lambda}{v}$ und $v = \frac{\mu}{v}$, so wird

$\alpha = -\frac{\lambda}{v^2}(\mu + \lambda\beta)$ sein, und man hat aus der Gleichung $\mu + \lambda\beta = v^2s$, in welcher β und s unbekannt sind, für s die kleinste ganze Zahl zu finden; oder man löse die Congruenz $\lambda\beta + \mu \equiv 0 \pmod{v^2}$ und benütze einen kleinen Werth von β .

Sind α und β bestimmt, so kann die Transformation [2] ausgeführt werden, wobei jedoch zu bemerken ist, dass in dieser Gleichung bei dem hier eingeschlagenen Gange der Rechnung die Coefficienten γ und ϵ stets Quadratzahlen sein müssen, daher [2] eigentlich so zu schreiben ist:

$$y^2 = (\alpha x + \beta)^2 - (\gamma^2 x + \delta)(\epsilon^2 x + \zeta) \quad [6]$$

Es kann nämlich, da b eine Primzahl bedeutet, der rechte Flügel in [1] d. i. $bx + c$ nur dann ein Quadrat werden, wenn für x ein Bruch gesetzt wird, dessen Nenner eine Quadratzahl

(also auch 1) oder b oder endlich ein Product dieser beiden Zahlen ist. Brüche der zwei letzten Arten können aus [1] in beliebiger Anzahl zwar augenblicklich gewonnen, für den vorliegenden Zweck aber desshalb nicht verwendet werden, weil sie die Ermittlung eines ganzzahligen Werthes für x von der Lösung einer quadratischen Congruenz nach dem Modul b abhängig machen würden, wie aus dem weiteren Verlaufe dieses Calculs zu ersehen ist. Um daher solche Werthe für x aus [2] nicht zu erhalten, wurde in dem Ausdrucke von α unter [3] der Factor b eliminirt und es bleiben somit für x nur Brüche mit quadratischem Nenner übrig; desshalb stehen in [6] die Coefficienten γ^2 und ε^2 .

Weil ferner die rechte Seite dieser Gleichung sich auf $bx + c$ reduciren muss, so ist $\alpha^2 x^2 = \gamma^2 \varepsilon^2 x^2$, also $\alpha = \gamma \varepsilon$ und $\frac{\alpha}{\gamma} = \varepsilon$.

Aus der jetzt fertigen Gleichung [6] fliesst sofort

$$x = \frac{-\delta}{\gamma^2}, \quad y = -\frac{\alpha\delta}{\gamma^2} + \beta = \frac{-\delta\varepsilon + \beta\gamma}{\gamma};$$

und wenn man den Zähler dieses Bruches mit x bezeichnet, so ist $y = \frac{x}{\gamma}$; setzt man diese Werthe in [1], so entsteht die identische Gleichung $\frac{x^2}{\gamma^2} = b\left(-\frac{\delta}{\gamma^2}\right) + c$, und zieht man diese von [1] ab, so kömmt die unbestimmte Gleichung

$$y^2 - \frac{x^2}{\gamma^2} = b\left(x + \frac{\delta}{\gamma^2}\right) \quad \text{oder} \quad \gamma^2 y^2 = b(\gamma^2 x + \delta) + x^2.$$

Lässt man $b(\gamma^2 x + \delta) + x^2 = \left(\frac{\gamma^2 x + \delta}{q} + x\right)^2$ sein, so folgt nach bewirkter Reduction $b = \frac{\gamma^2 x + \delta}{q^2} + \frac{2x}{q}$ und hieraus;

$$\gamma^2 x = bq^2 - 2xq - \delta; \quad [7]$$

diese Gleichung mit den Unbestimmten q und x kann fortan aus den für x und y gefundenen Brüchen unmittelbar gebildet werden.

Soll für x eine ganze Zahl resultiren, so muss in [7] die rechte Seite durch γ^2 theilbar sein, und der dies vermittelnde Werth von q ergibt sich aus der Congruenz

$$bq^2 - 2xq - \delta \equiv 0 \pmod{\gamma^2} \quad [8]$$

und liefert schliesslich, in [7] eingesetzt, den gesuchten ganzzahligen Werth von x .

Wären v_0 und w_0 vielziffrige Zahlen, wodurch die weitere Rechnung beschwerlich würde, so kann man mit diesen Werthen kleinere Zahlen für v und w aus der Gleichung [4] finden, wenn man ihr die Gestalt (II) im ersten Abschnitte verschafft und sich zu diesem Behufe der dortigen Gleichung (III) bedient. Dieser zufolge ist $w_0\alpha_1 + \beta_1 = v_0$ und α_1, β_1 sind die Unbekannten; bestimmt man diese in den kleinsten Zahlen und transformirt [4] so wird

$$v^2 = (\alpha_1 w + \beta_1)^2 + (\gamma_1 w + \delta_1)(\epsilon_1 w + \zeta_1);$$

und dieser Gleichung können für w und v mit weniger Ziffern geschriebene Werthe entnommen werden, die hierauf in [5] einzustellen sind.

1. Exempel. $y^2 = 1124 \pmod{20521}$

Der Modul ist ein quadratischer Rest von $1124 = 4.281$, somit liegt der Rechnung die Gleichung $y^2 = 20521x + 1124$ zu Grunde und es ist

$$\alpha = -\frac{20521w(v + \beta w)}{v^2 - 1124w^2};$$

$$v^2 = 1124w^2 + 20521, \quad v = 1124z + r$$

$$w^2 = 1124z^2 + 2rz - 18 + \frac{r^2 - 289}{1124};$$

$$r = 17, 579 \quad w^2 = 1124z^2 + 34z - 18 \quad (1)$$

$$B = 0, 298 \quad w^2 = 1224z^2 + 1158z + 280 \quad (2)$$

Setzt man in (1) $2z = z_0$, so folgt $w^2 = 281z_0^2 + 17z_0 - 18$; da sich hier ein ganzzahliges z_0 nicht sofort finden lässt, so bilde man aus dieser Gleichung nach (IV) für $\beta_1 = 0$ die derivirte $\Delta^2 = -72\alpha_1^2 + 20521$, $\Delta = 72z_1 + r_1$,

$$\alpha_1^2 = -72z_1^2 - 2r_1z_1 + 285 - \frac{r_1^2 - 1}{72}; \quad r_1 = 1, 17, 19, 35; \\ B = 0, 4, 5, 17;$$

man erhält nun das System der Gleichungen

$$\begin{aligned} \alpha_1^2 &= -72z_1^2 - 2z_1 + 285 \\ n &= \quad n - 34z_1 + 281 \\ n &= \quad n - 38z_1 + 280 \\ n &= \quad n - 70z_1 + 268. \end{aligned}$$

Für $z_1 = -2$ wird in der ersten Gleichung $\alpha_1 = 1$, somit ist $w^2 = z_0^2 + (40z_0 - 9)(7z_0 + 2)$ und $z_0 = -\frac{2}{7} = w$, $z = -\frac{1}{7}$,

$v = \frac{1005}{7}$; nun wird $\alpha = -\frac{2}{49}(1005 + 2\beta)$ und aus der Congruenz $1005 + 2\beta \equiv 0 \pmod{49}$ findet man $\beta = 12$, somit $\alpha = -42$ und $y^2 = (42x - 12)^2 - (441x + 20)(4x - 49)$; es ist daher

$x = \frac{49}{4}$, $y = \frac{1005}{2}$ und nach [7] $4x = 20521q^2 - 2010q + 49$, da das letzte Trinom durch 4 theilbar sein muss, so besteht nach Weglassung der Vielfachen von 4 die Congruenz $q^2 - 2q + 1 \equiv 0 \pmod{4}$; somit ist $q = 1$, $x = 4640$, $y = 9758$.

Hätte man die Gleichung (2) benützt, welche für $z = 2z_0$, $w = 2w_0$ und nach Kürzung durch 4 in $w_0^2 = 1124z_0^2 + 579z_0 + 70$ übergeht, so stösst man auch hier auf kein ganzzahliges z_0 ; daher nach (VI) $L^2 = 70\Delta^2 + 20521(\beta_1^2 - 70)$; für $\beta_1 = 4$, $L = 3l$, $\Delta = 3d$ wird nach Division durch 9: $l^2 = 70d^2 - 123126$; $l = 70z_1 + r_1$;

$$d^2 = 70z_1^2 + 2r_1z_1 + 1759 + \frac{r_1^2 - 4}{70}; \quad r_1 = 2, 12 \\ B = 0, 2$$

also $d^2 = 70z_1^2 + 4z_1 + 1759$ und $d^2 = 70z_1^2 + 24z_1 + 1761$, die erste dieser Gleichungen, gibt für $z_1 = 3$: $d = 49$, $l = 212$, $L = 636$; für $\beta_1 = -4$ wird $\alpha_1 = -12$,

$w_0^2 = (12z_0 + 4)^2 + (28z_0 + 9)(35z_0 + 6)$; also $z_0 = -\frac{9}{28}$,

$w_0 = \frac{1}{7}$; $z = -\frac{9}{14}$, $w = \frac{2}{7}$, $v = \frac{1005}{7}$, wie oben.

2. Exempel. $y^2 \equiv 16315 \pmod{21433}$

Der Modul 21433 ist ein quadratischer Rest von $16315 - 21433 = -5118 = -2.3.853$, daher bildet die Gleichung $y^2 = 21433x - 5118$ die Grundlage der Rechnung und $\alpha = -\frac{21433w(v + \beta w)}{v + 5118w^2}$

$$v^2 = -5118w^2 + 21433; \text{ für } w = 2 \text{ wird } v = 31,$$

$$\alpha = -2(31 + 2\beta); \beta = -16, \alpha = 2 \text{ und}$$

$$y^2 = (2x - 16)^2 - (x - 5374)(4x - 1), \text{ somit } x = 5374, y = 10732.$$

3. Exempel. $y^2 \equiv 127 \pmod{239}$.

Der Modul ist kein quadratischer Rest von 127, wohl aber ist -239 ein quadratischer Rest von $127 + 239 = 366 = 2.3.61$; also dient als Ausgangspunkt die Gleichung

$$y^2 = 239x + 366 \text{ und } \alpha = -\frac{239w(v + \beta w)}{v^2 - 366w^2};$$

$$v^2 = 366w^2 - 239; v = 366z + r,$$

$$w^2 = 366z^2 + 2rz + \frac{r^2 + 239}{366}; \quad r = 35 \quad B = 4$$

$$w^2 = 366z^2 + 70z + 4, \text{ für } z = 0 \text{ wird } w = 2, v = 35$$

$$\alpha = 2(35 + 2\beta), \beta = -17, \alpha = 2,$$

$$y^2 = (2x - 17)^2 - (x - 77)(4x + 1) \text{ und } x = 77, y = 137.$$

4. Exempel. $y^2 \equiv 4163 \pmod{19139}$

Der Modul ist ein quadratischer Rest von $d - 2b = -34115 = -5.6823$, somit ist $y^2 = 19139x - 34115$ die erste Grundgleichung und

$$\alpha = -\frac{19139w(v + \beta w)}{v^2 + 34115w^2}; v^2 = -34115w^2 + 19139,$$

$$v = 34115z + r, w^2 = -34115z^2 - 2rz - \frac{r^2 - 19139}{34115};$$

$$r^2 \equiv 19139 \pmod{6823.5}, \quad r^2 \equiv 19139 \pmod{6823};$$

der Modul 6823 ist ein quadratischer Rest von

$$19139 - 2.6823 = 5493, \text{ somit } r^2 = 6823\rho + 5493$$

die zweite Grundgleichung und

$$\alpha_1 = -\frac{6823 w_1 (r_1 + \beta_1 w_1)}{v_1^2 - 5493 w_1^2}; \quad v_1^2 = 5493 w_1^2 + 6823,$$

$$v_1 = 5493 z_1 + r_1, \quad w_1^2 = 5493 z_1^2 + 2r_1 z_1 - 1 + \frac{r_1^2 - 1330}{5493};$$

$r_1^2 \equiv 1330 \pmod{1831.3}$; hier ist $r_1^2 \equiv 1831\rho_1 + 1330$ die dritte Grundgleichung und

$$\alpha_{..} = -\frac{1831 w_{..} (v_{..} + \beta_{..} w_{..})}{v_{..}^2 - 1330 w_{..}^2}; \quad v_{..}^2 = 1330 w_{..}^2 + 1831,$$

$$v_{..}^2 = 1330 z_{..} + r_{..},$$

$$w_{..}^2 = 1330 z_{..}^2 + 2r_{..} z_{..} - 1 + \frac{r_{..}^2 - 501}{1330}; \quad r_{..}^2 \equiv 501 \pmod{2.5.7.19}$$

somit $r_{..} = 201, 331, 369, 429$ und $w_{..}^2 = 1330 z_{..}^2 + 662 z_{..} + 81$;
 $B = 30, 82, 102, 138$

für $z_{..} = 0$ wird $w_{..} = 9, \quad v_{..} = 331, \quad \alpha_{..} = -9(331 + 9\beta_{..})$;
 $\beta_{..} = -36, \quad \alpha_{..} = -63$ und

$$r_1^2 = (63\rho_1 + 36)^2 - (49\rho_1 + 34)(81\rho_1 - 1), \quad \text{somit } \rho_1 = -\frac{34}{49},$$

$r_1 = \frac{54}{7}$ und $49\rho_1 = 1831p^2 - 108p - 34 \equiv 0 \pmod{49}$ oder
 $(p-3)^2 \equiv 0 \pmod{49}$, also $p = 3, \rho_1 = 329$ und $r_1 \equiv 777 \pmod{5493}$;

daher $r_1 = 1054, 2608$ und $w_1^2 = 5493 z_1^2 + 2108 z_1 + 201$ (1),
 $B = 202, 1238$ und $w_1^2 = 5493 z_1^2 + 5216 z_1 + 1237$ (2),
 in (1) ist $z_1 = 4n$, bis $z_1 = 20$ findet sich nichts! (2) ist in
 ganzen Zahlen unmöglich.

Aus (1) folgt: $L^2 = 201\Delta^2 + 4.6823(\beta_0^2 - 201)$; $\beta_0 = 15$,
 $L = 4l, \Delta = 4d$, durch 16 dividirt:

$$l^2 = 201d^2 + 40938; \quad l = 201z_0 + r_0;$$

$$d^2 = 201z_0^2 + 2r_0z_0 - 203 + \frac{r_0^2 - 135}{201}; \quad r_0 = 66$$

$$B = 21$$

$d^2 = 201z_0^2 + 132z_0 - 182$; in ganzen Zahlen unmöglich; somit $L_1^2 = -182\Delta_1^2 + 24.6823(\beta_2^2 + 182)$, $\beta_2 = 2$, $L_1 = 4l$, $\Delta_1 = 4d$ durch 16 dividirt:

$$l_1^2 = -182d_1^2 + 1903617; l_1 = 182z_2 + r_2;$$

$$d_1^2 = -182z_2^2 - 2r_2z_2 + 10459 - \frac{r_2^2 - 79}{182}; r_2 = 25, 53 \\ B = 3, 15$$

$$\text{hiemit } d_1^2 = -182z_2^2 - 50z_2 + 10456 \text{ und} \\ d_1^2 = -182z_2^2 - 106z_2 + 10444$$

die erste dieser Gleichungen liefert für $z_2 = -4$, $d_1 = 88$, $l_1 = -703$, $L_1 = -2812$, $\alpha_2 = 7$ und

$$d^2 = (7z_0 + 2)^2 + 2(2z_0 + 3)(38z_0 - 31);$$

$$z_0 = -\frac{3}{2}, d = -\frac{19}{2}, l = -\frac{471}{2}, L = -942;$$

für $\beta_0 = -15$ wird $\alpha_0 = -81$,

$$w_1^2 = (81z_1 + 15)^2 - 2(89z_1 + 12)(6z_1 + 1); \text{ somit } z_1 = -\frac{1}{6},$$

$$w_1 = \frac{3}{2}, v_1 = \frac{277}{2}, \alpha_1 = -\frac{3}{4}(277 + 3\beta_1), \beta_1 = -91, \alpha_1 = -3$$

und $r^2 = (3\rho + 91)^2 - (\rho - 697)(9\rho - 4)$; $\rho = 697$, und $r \equiv 2182 \pmod{6823}$, somit

$$r = 2182, 15828; w^2 = -34115z^2 - 4364z - 139 \quad (1)$$

$$B = 139, 7343; w^2 = -34115z^2 - 31656z - 7343 \quad (2)$$

in ganzen Zahlen unmöglich.

Somit aus (1) $L_{..}^2 = -139\Delta_{..}^2 + 4.19139(\beta_3^2 + 139)$; $\beta_3 = 1$, $L_{..} = 4l_{..}$, $\Delta_{..} = 4d_{..}$ und durch 16 abgekürzt,

$$l_{..}^2 = -139d_{..}^2 + 669865; l_{..} = 139z_3 + r_3,$$

$$d_{..}^2 = -139z_3^2 - 2r_3z_3 + 4819 - \frac{r_3^2 - 24}{139}; r_3 = 21 \\ B = 3'$$

$$d_{..}^2 = -139z_3^2 - 42z_3 + 4816;$$

da hier z_3 gerade sein muss, so setze man $d_{..} = 2d_{...}$, $z_3 = 2z_4$ und dividire durch 4 $d_{...}^2 = -139z_4^2 - 21z_4 + 1204$; für $z_4 = -3$

wird $d_{,,} = 4$, $z_3 = -6$, $l_{,,} = -813$, $L_{,,} = -3252$, für $\beta_1 = -1$ wird $\alpha_1 = -4$, somit

$$w^2 = (4z + 1)^2 - (1101z + 70)(31z + 2) \text{ und } z = -\frac{2}{31},$$

$w = \frac{23}{31}$, $v = \frac{588}{31}$, $\alpha = -\frac{23}{31^2}(588 + 23\beta)$; für $\beta = 58$ ist $\alpha = -46$ und $y^2 = (46x - 58)^2 - (4x - 39)(529x - 961)$, also $x = \frac{39}{4}$, $y = \frac{781}{2}$ und $4x = 19139q^2 - 1562q + 39 \equiv 0 \pmod{4}$, oder $(q + 1)^2 \equiv 0 \pmod{4}$, somit $s = +1$, $x = 4404$, $y = 9179$.
