Diophantische Gleichungen

(1) a**x + by = 1** , a,b,x,y $\in \mathbb{Z}$. Gesucht: x, y
Zur Lösbarkeit sind a, b notwendig und hinreichend teilerfremd.
Allgemeine Lösung: **x** = u + b·n , **y** =v - a·n , n $\in \mathbb{Z}$
Für die spezielle Lösung (u, v) benutzt man den erweiterten Euklidischn Algorithmus oder ermitelt den ersten Näherungsbruch: a/b ≈ a'/b', z. B. durch Kettenbruch, siehe Bsp. 1
Fall 1: a·b' + b·(-a') = 1 → **u = b' , v = -a'** spez. Lösung mit n = 0
Fall 2: a·b' + b·(-a') = -1
a·(-b') + b·a' = 1
spezielle Lösung u_= -b', v_= a' mit n = 0
Für spez. Lösung mit u>0 wähle mit n=1: **u = b - b' , v = -a + a'**

(2) a**x + by = c** , a,b,c,x,y $\in \mathbb{Z}$. Genau dann lösbar wenn ggT(a,b) | c
Äauivalent beschrieben durch die Kongruenz ax ≡ c mod b
a, b seien bereits teilerfremd, also c = c_{alt}/ggT(a,b) [ggT... größter gemeinsamer Teiler]
$ax_1 + by_1 = 1$ hat die spez. Lösung u_1 und v_1. Somit ist u = c·u_1 und v = c·v_1.
Allgemeine Lösung wie oben.

Das Programm ermittelt eine spezielle Lösung mit der **Funktion dio(a, b [, c, p])**
Wird c nicht angegeben oder "c" eingegeben, ist c = ggT(a,b)>0.
p={1 ; 2}: x bzw. y hat kleinsten Wert>0. Liefern beide Einstellungen das gleiche Ergebnis, dann gibt es nur eine positive Lösung.
Andere Zahlen p errechnen spezielle Lösungen mit Parameter n = p.

Beispiel 1
80x + 43y = 1

$$\frac{43}{80} = \frac{1}{1+\frac{37}{43}} = \frac{1}{1+\frac{1}{1+\frac{6}{37}}} = \frac{1}{1+\frac{1}{1+\frac{1}{6+\frac{1}{6}}}} \approx \frac{1}{1+\frac{1}{1+\frac{1}{6}}} = \frac{7}{13}$$

Der reduzierte Kettenbruch von 80/43 liefert den ersten Näherungsbruch 80/43 ≈ 13/7
80·7 + 43·(-13) = 1 → spezielle Lösung u = 7 , v = -13. Eingabe dio(80,43)
Allgemeine Lösung: **x** = 7 + 43n ; **y** = -13 -80n , n $\in \mathbb{Z}$ in allen Bsp.

Beispiel 2
65x + 72y = 1
Näherungsbruch 65/72 ≈ 28/31
65·31 + 72·(-28) = -1 → Fall 2
65·(-31) + 72·28 = 1.
Für n = 0 ist u_ = -31 , v_ = 28. n=1 liefert
u = 72·1 + u_ = 72 - 31 = b - b' = **41**
v = -65·1 + v_ = 28 - 65 = a' - a = **-37**
Eingabe dio(65,72,1,1)
Allg. Lösung: **x** = 72n + 41 ; **y** = -65n - 37
Mit n=0 erhält man 65·41 -72·37 = 1

Beispiel 2a mit a>b
17x + 13y = 1
17/13 ≈ 4/3
17·3 + 13·(-4) = -1
u_ = -3 , v_ = 4
u = 13 - 3 = **10**
v = 4 - 17 = **-13**
…
17·10 - 13·13 = 1
Eingabe dio(17,13,1,1)

Beispiel 3 (c > 1)
Ein Rohstoff liegt in Dosierungen von 24 g sowie 35 g vor. Wie viele jeder Art sind zu verwenden, um genau 1 kg davon zu erhalten?
$24x + 35y = 1000$. Betrachte zunächst
$24x_1 + 35y_1 = 1$
$24/35 \approx 11/16$ als Näherungsbruch
$24*16-11*35 = -1$
$x_1 = -16 + n\cdot 35$, $y_1 = 11 - n\cdot 24$ und somit
$x = -16000 + n\cdot 35$, $y = 11000 - n\cdot 24$
$x > 0 : n>457$; $y > 0: x < 459 \rightarrow n=458$
Es gibt eine einzige positive Lösung (u | v) = (30 | 8)
Eingabe: dio(24,35,1000,1) und dio(24,35,1000,2) liefern beide dieses Ergebnis.
Bemerkung: Bei Dosen 24 g und 45 g geht es nicht, da ggT(24,45) nicht 1000 teilt.

Beispiel 4
Der öffentliche Schlüssel eines RSA-Systems sei (N, e) = (247, 11). Der code C=3 soll entschlüsselt werden.
Die Eingabe von N = 247 liefert die Primfaktorzerlegung p*q = 13 * 19.
N' = φ(N) = (p-1)(q-1) = 12·18 = 216. ggT(N', e) = ggt(216,11) = 1.
{Ebenso ist dio(11,216) = dio(11,216,1).}
$d\cdot e \equiv 1 \bmod N' \rightarrow d \cdot e + k \cdot N' = 1$
Für d ermitteln wir dio(11,216,1,1) = (59,-3), **d = 59** oder allgemein $d \equiv 59 \bmod 216$.
Die Botschaft: $B \equiv C^d \bmod N$
$B = 3^{59} \bmod 247 =$ **243**
$3^8 \equiv 139 \bmod N$, $3^{16} \equiv 139^2 \bmod N \equiv 55 \bmod N$, $3^{32} \equiv 55^2 \bmod N \equiv 61 \bmod N$.
Mit ggT(C, N) = 1 ist $3^{59} \equiv 61\cdot 3^{27} \bmod N \equiv (61\cdot 55)\cdot(139\cdot 27) \bmod N \equiv 144\cdot 48 \bmod N$
$\equiv 243 \bmod N$

Beispiel 5 (negative Koeffizienten)
Ein Verein gibt für jedes Mitglied 2 EUR aus, während mehr als die Hälfte der Mitglieder 5 EUR einzahlen. Insgesamt verbessert sich die Kasse dabei um 30 EUR.
Wie viele Mitglieder (x) zählt der Verein höchstens?
(1) $-2x + 5y = 30$
dio(-2,5,30,1) $\rightarrow x = 5 +5\cdot k$; $y = 8 +2\cdot k$ $(k \in Z)$
(2) $x < 2y$
$5 + 5k < 16 + 4k$
$k < 11$
k = 10 ergibt die Höchstzahl von x = **55** Mitgliedern bei y = 28 Einzahlern.
Proben: $-2\cdot 55 + 5\cdot 28 = 30$ und $55 > 2\cdot 28$. k = 11 verletzte Bedingung (2).
Die **Mindestzahl** der Mitglieder beträgt 10 bei maximaler Einzahlbereitschaft (k=1).

Änderung der Problemstellung (Beispiel 5a):
Der Kassenwart behauptet bei obigen Zahlungsvorgängen, dass die Kasse um 13 EUR geschmälert wurde. Ist das möglich?
dio(-2,5,-13,2) $\rightarrow x = 9 +5\cdot k$; $y = 1 +2\cdot k$ $(k \in Z)$
Die über doppelt so große Mitgliedezahl wächst über das Doppelte an und aus (2) folgt
$9+5k < 2+4k$
$k < -7$. Das ergäbe negative Mitgliederzahlen. Der Kassenwart hat sich also bestenfalls geirrt.

Beispiel 6 (Zusammenhang mit Kongruenzen)
An 20 Personen sollen Pralinen aus Schachteln mit je 12 Stück fair (also gleichmäßig) verteilt werden, so dass 6 Stück übrig bleiben. Geht das?
x... Anzahl der Schachteln
$12x \equiv 6 \mod 20$ ist äquivalent zu der Gleichung
$12x + 20y = 6$.
Lösbar, wenn 6 | ggT(12,20). Da 6 : 4 nicht teilbar ist, müssen wohl 2 Pralinen vernascht werden bei folgender

Änderung des Problems: Es sollen 8 Stück übrig bleiben (statt 6):
$12x \equiv 8 \mod 20$
$3x \equiv 2 \mod 5$ ist äquivalent zu der Gleichung
$3x + 5y = 2$
Eingabe dio(3,5,2) oder dio(12,20,8) →
x = 4 Schachteln ergeben für jede der 20 Personen y = 2 Pralinen mit Rest 8.
Die allgemeine Lösung
$x = 4 + 5n$ ist äquivalent zu $x \equiv 4 \mod 5$.

Beispiel 7 (2x2-System von Kongruenzen)
Teilt man eine Anzahl Äpfel unter 13 Personen auf, bleiben 2 übrig. Teilt man sie unter 19 Personen auf, bleiben 14 übrig.
$x \equiv 2 \mod 13$
$x \equiv 14 \mod 19 \equiv -5 \mod 19$
$x - 13y = 2$
$x - 19z = -5$
Subtraktion ergibt die diophantische Gleichung
$-13y + 19z = 7$
dio(-13,19,7,1) liefert die spezielle Lösung
y=17 , z=12 und eine Lösung
$x = 2+13\cdot17 = -5+19\cdot12 =$ **223** Äpfel.
Probe: 223/13 = $17\ ^{2}/_{13}$ und 223/19 = $11\ ^{14}/_{19}$
Wegen ggT(13, 19) = 1 sind alle positiven Lösungen $x = 223 + n\cdot(13\cdot19)$, $n \in \mathbb{Z}$, $n \geq 0$.
Unabhängig vom Sachverhalt ist die allgemeine Lösung somit $x \equiv 223 \mod (13\cdot19)$.
Die Lösung größerer Systeme ist bei Wikipedia erklärt im Kapitel *Chinesischer Restsatz*.

Beispiel 8 (2 Gleichungen)
Jemand hat 30 Vögel für 30 Münzen gekauft.
Für 3 Spatzen zahlte er eine Münze, für zwei Wildtauben ebenfalls eine Münze und für jede Taube zwei Münzen.
Wie viele Vögel jeder Art hat er gekauft ? *Aufgabe von FIBONACCI (1180 - 1240)*

$a + b + c = 30$	| *2
$2a + 2b + 2c = 60$	(1)
$a/3 + b/2 + 2c = 30$	| *6
$2a + 3b + 12c = 180$	(2)

(2) - (1) liefert
$b + 10c = 120$
$b = 10\cdot(12 - c)$ liefert die spez. Lösungen (10 | 11) und (20 | 10).
Wegen a>0 ist **b=10, c=11, a=9** . Geliefert von dio(1,10,120,1).