Диофантови уравнения

Когато решенията на дадено уравнение се търсят в множество на целите числа, казваме, че решаваме диофантово уравнение (ДУ). Тук ще разглеждаме само ДУ от вида $p(x_1,x_2,...,x_N)=0$, където p е полином с цели коефициенти.

За разлика от решаването на обикновени уравнения с едно неизвестно, решаването на ДУ с едно неизвестно не е сериозен информатичен проблем. Наистина, ако имаме уравнението $a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n=0$, то от записа $(a_0x^{n-1}+a_1x^{n-2}+...+a_{n-1})x= -a_n$ става ясно, че x е делител на a_n (числото в скобите е цяло) и задачата се свежда до изчерпване. По-интересни като ДУ са уравненията с две неизвестни (които пък като обикновени не представляват интерес). Оказва се, че диофантовостта, макар да не може да изиграе ролята на второ уравнение, все пак доста ограничава класа от решения на такива уравнения.

ДУ от първа степен с две неизвестни

Уравнението има вида ax + by = c. Очевидно, ако d е общ делител на a и b и ако d не дели c, уравнението няма да има решение (лявата част се дели на d, а дясната – не). Оказва се, че това необходимо условие е и достатъчно.

Нека (x_0, y_0) е едно решение на това уравнение. Тогава всички числа от вида $x=x_0+bt$, $y=y_0-at$, където t е произволно цяло число, също са решения – доказателството е просто заместване. Не е особено трудно да се покаже (с допускане на противното, например), че това е и единственият клас от двойки, които удовлетворяват уравнението.

Единственият проблем тогава остава намирането на едно (“начално”) решение на такива ДУ. Има различни алгоритми за това, но тук ще използваме алгоритъм, свързан с представянето на числа във вид на верижни дроби.

Числото $a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots}}}}$, където a_i са естествени числа (с единствено евентуално изключение $a_0=0$), се нарича “верижна дроб”. Очевидно, дробта е определена в този си вид от редицата $\{a_0, a_1, a_2, ...\}$. Ако тази редица е крайна, и дробта се нарича “крайна”.

Ако е дадено рационалното число $f=\frac{p}{q}$, където, без ограничение на общността, p и q са естествени, лесно можем да съобразим и алгоритъм за превръщане на f в крайна верижна дроб. Например $\frac{1}{5}$ вече има този вид ($\{0, 5\}$), 7 – също лесно се представя като $\{7\}$. За $\frac{2}{3}$ това не е така, но можем да направим следните преобразования: $\frac{2}{3}=\frac{1}{\frac{3}{2}}=\frac{1}{1+\frac{1}{2}}=0+\frac{1}{1+\frac{1}{2}}=\{0,1,2\}$. Алгоритъмът е ясен: отделяме цялата част, а оставащата правилна дроб представяме като реципрочна на реципрочната. Последната от своя страна ще е неправилна и процесът се повтаря до получаване на дроб с числител 1. Единственият особен случай е, когато самото f е цяло, но тогава то просто вече има нужния вид. Този процес е краен при рационални f (и само при тях).

Задача: Нека е дадена двойка естествени числа p и q. Намерете представянето на дробта p/q във вид на верижна дроб.

ВХОД: От стандартното входно устройство се въвежда един ред с естествените числа p и q, разделени с интервал. Никое от числата няма повече от 18 цифри.

ИЗХОД: Запишете на стандартното изходно устройство на един ред, разделени с по един интервал, членовете на редицата от естествени (с евентуално изключение на първия елемент, който може да е 0) числа, която определя верижното представяне на p/q.

ПРИМЕРЕН ВХОД: `215 37`

СЪОТВЕТЕН ИЗХОД: `5 1 4 3 2`

Верижните дроби имат отношение към намирането на началното решение на ДУ от първа степен в следния аспект. Ако премахнем последния член на редицата, която представя една дроб p/q във верижна, ще получим нова крайна верижна дроб. Тя представя рационалното число p’/q’, което лесно можем да получим, като извършим действията. Случаи, при който този процес не е ясен, са:

- когато q=1, при което p/q е цяло и има само едно звено. В този случай ще положим p’=1, q’=0;
- когато p’ = 0, полагаме q’ = 1.

Теоремата, върху която ще изградим алгоритъма, гласи: $|p.q'-q.p'| = 1$.

Разглеждаме диофантовото уравнение от първа степен с две неизвестни ax + by = c. Да образуваме дробта f = |a/b|. Преобразуваме f във верижна дроб, премахваме последното звено и по правилата по-горе образуваме

дробта p'/q'. Съгласно цитираната теорема ||a|q' – |b|p'| = 1. Можем да пишем още |a|q'-|b|p'=ε, което е 1 или -1. Ако със sgn(d) означим "знака на d" (1, ако d≥0 и –1 при d<0), то |d|=d.sgn(d). Тогава имаме a.sgn(a).p'+b.(-sgn(b)).q' = ε, от което след умножаване с εc от двете страни получаваме a.[sgn(a).p'.εc] +b.[(-sgn(b)).q'.εc] = c и x_0 = ε.sgn(a).p'.c, y_0 = -ε.sgn(b).q'.c. Нека не забравяме, че всички тези действия ще дадат резултат само ако уравнението има клас от решения, както изисква необходимото и достатъчно условие.

Задача: Дадено е диофантовото уравнение от първа степен с две неизвестни ax + by = c. Да се намери броят на неговите решения (x, y), за които $d_1 \le x \le d_2$ и $d_3 \le y \le d_4$. За целите числа d_i имаме $d_1 \le d_2$ и $d_3 \le d_4$.

ВХОД: От стандартното входно устройство се въвеждат следните цели числа, като никое от тях няма повече от 20 цифри:

- ред 1: a, b и c, разделени с интервал;
- ред 2: d_1, d_2. d_3 и d_4, разделени с интервал.

ИЗХОД: Запишете на стандартното изходно устройство един ред с броя на намерените решения (0, ако решения няма).

ПРИМЕРЕН ВХОД:

```
2 -1 5
-10 10 -6 10
```

СЪОТВЕТЕН ИЗХОД:

```
8
```

Уравнения с повече от едно неизвестно от по-висока степен

За такива уравнения не се знае изобщо много, но има класове, които са изследвани добре.

1. ДУ от вида $x^2 + y^2 = z^2$ ("Питагорови тройки"). Всички взаимно прости питагорови тройки се получават с формулите x = uv, $y = (u^2-v^2)/2$, $z = (u^2+v^2)/2$, където u и v са нечетни и взаимно прости естествени параметри. Останалите решения се получават, като се умножи всеки елемент на някоя от тези тройки с едно и също естествено число и се варират знаците.
2. Уравнения на Пел с общ вид $x^2 - Ay^2 = 1$, където A е цяло. Тривиалните случаи са A≤0 и $A = t^2$, където t е естествено число. За случаите, в които A>0 и A не е точен квадрат е доказано, че образуват безкраен клас от двойки. В този случай за намирането на всички решения ни е нужна такава двойка (x_0,y_0), за което $x_0>0$, $y_0>0$ и $x_0 + y_0\sqrt{A}$ е минимално (наричаме тази двойка *най-малко решение*). Тогава всички решения имат вида $(\pm x_n, \pm y_n)$, където n е неотрицателно цяло и

   За намирането на най-малкото решение могат да се използват изчерпващи алгоритми. Ако развием

$$\begin{cases} x_n = \frac{1}{2}\left[\left(x_0 + y_0\sqrt{A}\right)^n + \left(x_0 - y_0\sqrt{A}\right)^n\right] \\ y_n = \frac{1}{2\sqrt{A}}\left[\left(x_0 + y_0\sqrt{A}\right)^n - \left(x_0 - y_0\sqrt{A}\right)^n\right] \end{cases}$$

   числото $\sqrt{A}$ във верижна дроб (по същия алгоритъм като по-горе, само че дробта ще бъде ***безкрайна периодична***) можем да намерим нетривиални решения на уравнението на Пел. Опитайте се да установите как и какви.
3. За по-общото уравнение $x^2 - Ay^2 = C$, където A и C са цели се знае че:
   - ако има поне едно решение (x_0, y_0), то има и безброй много решения;
   - ако (u_n, v_n) са решенията на уравнението на Пел $u^2 - Av^2 = 1$, то двойките (x, y), за които $x=x_0u_n+Ay_0v_n$ и $y=x_0u_n+y_0v_n$ също са решения на даденото уравнение;
   - нужен е краен брой начални решения като горното (x_0, y_0) и преобразованията по-горе, за да опишем всички решения на уравнението;
   - липсата на решение на уравнението често се доказва с липсата на решение на сравнението $x^2-Ay^2 \equiv C$ по някакви модули. 4 и 8 са много използвани модули, но изобщо никак не е лесно да се определи подходящият модул.
4. Решаването на най-общите ДУ от втора степен с вид $Ax^2+Bxy+Cy^2+Dx+Ey+F=0$ с подходящи полагания (какви?) води до решаването на уравненията, описани в предната точка.
5. С много малки изключения, уравненията с две неизвестни от по-висока степен могат да имат само краен брой решения. Едно класическо изключение е $x^4+y^2=z^2$. Намерете вида на всички негови решения.
6. Голямата теорема на Ферма гласи, че уравнението $x^n+y^n=z^n$ няма ненулеви решения за n>2. Едно доказателство, направено през 1984 и уточнявано десетина години след това засега се проверява. С компютър не са намерени противоречия за обозрими стойности.