Diofantiska ekvationer

De ekvationer vi ska behandla är av typen

$$ax + by = c$$

där a, b, c är givna heltal och man bara är intresserad av heltalslösningar, d.v.s. x och y ska vara heltal. Vissa sådana ekvationer saknar lösningar.

Exempel. Ekvationen $35x + 55y = 102$ har ingen lösning. Oavsett vilka värden man ger x och y kommer VL att vara delbart med 5. Men 102 är inte delbart med 5.

Ett nödvändigt villkor för att det ska finnas en lösning är alltså att SGD(a, b) delar c. Om detta villkor är uppfyllt kan man dividera bägge sidor av ekvationen med SGD(a, b) utan att ändra lösningsmängden. Om man gör denna division kommer SGD av koefficienterna i VL att bli 1. I fortsättningen antar vi att SGD$(a, b) = 1$. Vi ska se att i detta fall har ekvationen alltid oändligt många lösningar. Antag att vi har hittat en lösning $x = x_0, y = y_0$. Om $x = x_1, y = y_1$ är en annan lösning gl̈ler alltså att $ax_0 + by_0 = c$ och $ax_1 + by_1 = c$. Detta ger att $a(x_1 - x_0) + b(y_1 - y_0) = 0$. Vi får alltså den nya lösningen (x_1, y_1) genom att till den gamla (x_0, y_0) addera (x_1-x_0, y_1-y_0), som är en lösning till ekvationen $ax+by = 0$. Omvänt, om (x_0, y_0) är en lösning till ekvationen $ax+by = c$ och (x', y') är en lösning till ekvationen $ax+by = 0$, så kommer (x_0+x', y_0+y') att vara en lösning till ekvationen $ax + by = c$, för $a(x_0 + x') + b(y_0 + y') = (ax_0 + by_0) + (ax' + by') = c + 0 = c$. Vi kan alltså ta reda på ALLA lösningar till ekvationen $ax + by = c$ genom att hitta EN lösning (en partikulärlösning) till denna ekvation och till denna lösning addera ALLA lösningar till motsvarande "homogena" ekvation $ax + by = 0$. Ibland kan man se en partikulärlösning utan räkning. T.ex. har ekvationen $7x + 34y = 1$ lösningen $x = 5, y = -1$ och ekvationen $34x + 37y = 3$ lösningen $x = -1, y = 1$. En metod som alltid fungerar är att hitta en lösning till $ax + by = 1$ genom Euklides algoritm baklänges (se boken) och sedan multiplicera denna lösning med c.

Exempel. Betrakta ekvationen $34x + 37y = 3$ och hjälpekvationen $34x + 37y = 1$. Vi bestämmer SGD$(34, 37)$ med Euklides algoritm.

$$37 = 1 \cdot 34 + 3$$

$$34 = 11 \cdot 3 + 1$$

Den sista likheten ger $1 = 34 - 11 \cdot 3$ och den första ger $3 = 37 - 34$, vilket ger $1 = 34 - 11(37 - 34) = 12 \cdot 34 - 11 \cdot 37$. Hjälpekvationen har alltså en lösning $x = 12, y = -11$, så den ursprungliga ekvationen har en lösning $x = 36 = 3 \cdot 12, y = -33 = 3 \cdot (-11)$.

Det återstår att bestämma den allmänna lösningen till $ax+by = 0$ där SGD$(a, b) = 1$. Om $ax = -by$ och SGD$(a, b) = 1$ måste a dela y (se nedan), så $y = ka$ för något heltal k. Detta ger $x = -kb$, så den allmänna lösningen till $ax + by = 0$ blir $x = -kb, y = ka$, där k är ett godtyckligt heltal.

Exempel. Ekvationen $34x + 37y = 0$ har allmänna lösningen $x = -37k, y = 34k$, så ekvationen $34x + 37y = 3$ har allmän lösning $x = 36 - 37k, y = -33 + 34k$, där k är ett godtyckligt heltal.

I resonemanget ovan användes följande: Om $ax = -by$ för några heltal a, x, b, y och $\text{SGD}(a, b) = 1$, så måste a dela y. Det kan inses på följande sätt. Gör en primfaktoruppdelning av a, x, b, y. Eftersom primfaktoruppdelningen av ett heltal är unik bortsett från ordningen av faktorerna och tecken på dem, så måste precis samma faktorer ingå i ax som i by. Men a och b har inga gemensamma primfaktorer eftersom $\text{SGD}(a, b) = 1$, så alla primfaktorer i a måste finnas i y, d.v.s. a delar y. Alternativt kan man resonera så här: Eftersom $\text{SGD}(a, b) = 1$ finns tal m och n så $ma + nb = 1$. Detta ger $may + nby = y$. Eftersom a delar både may och nby (a delar ju by), så delar a summan, d.v.s. a delar y.

Observera likheten i resonemanget ovan med det för lösning av linjära differentialekvationer. För att lösa t.ex. ekvationen $y'' + 3y' + 4y = x$ bestämmer man först EN lösning (en partikulärlösning), och adderar till den den allmänna lösningen till den homogena ekvationen $y'' + 3y' + 4y = 0$. På motsvarande sätt kan man lösa linjära ekvationssystem $AX = B$. Man kan först bestämma EN lösning och till den addera ALLA lösningar till $AX = 0$. (För linjära ekvationssystem brukar man inte göra så, eftersom det är lika lätt att direkt lösa det inhomogena ekvationssystemet.)