On a transformation of Lagrange

Keith Matthews

October 12, 2015

At the end of a memoir in 1770, Lagrange [3, pp. 717–726] gave a method for finding the solutions of a positive definite binary form equation

$$bt^2 + ctu + du^2 = a, \tag{0.1}$$

where $\gcd(t, u) = 1, \gcd(b, c, d) = 1 = \gcd(b, a), c^2 - 4bd < 0, b > 0, a > 0$. Then $\gcd(u, a) = 1$ and hence the congruence $\theta u \equiv t \pmod{a}$ has a unique solution θ in the range $-a/2 < \theta \leq a/2$. Then

$$\begin{aligned} bt^2 + ctu + du^2 &\equiv 0 \pmod{a} \\ b(\theta u)^2 + c(\theta u)u + du^2 &\equiv 0 \pmod{a} \\ b\theta^2 + c\theta + d &\equiv 0 \pmod{a}. \end{aligned}$$

The transformation

$$t = \theta u - ay \tag{0.2}$$

was used by Lagrange ([3, p. 700]) to convert equation (0.1) to

$$Pu^2 + Quy + Ry^2 = 1, \tag{0.3}$$

where $P = (b\theta^2 + c\theta + d)/a, Q = -(2b\theta + c), R = ab$.

(We remark that if (u, y) is a solution of (0.3), then $(t, u) = (\theta u - ay, u)$ is a solution of (0.1) with $\gcd(t, u) = 1$.)

We note that $D = c^2 - 4bd = Q^2 - 4PR$. Clearly if (u, y) is a solution of (0.3), so is $(-u, -y)$. There exists a transformation $u = \alpha X + \beta Y, y = \gamma X + \delta Y, \alpha\delta - \beta\gamma = 1$ such that

$$Pu^2 + Quy + Ry^2 = AX^2 + BXY + CY^2,$$

where the form (A, B, C) is reduced; i.e., $-A < B \leq A \leq C$ and where $A = C$ implies $B \geq 0$.

Lemma 0.1. *If $F(X,Y) = AX^2 + BXY + CY^2$ is a reduced positive definite form, then A is the minimum value of $F(X,Y)$ over integer pairs (X,Y) not both zero. Moreover*

(a) If $A < C$, the minimum is attained only at $\pm(1,0)$;

(b) If $A = C$ and $B < A$, the minimum is attained only at $\pm(1,0)$ and $\pm(0,1)$;

(c) If $A = C = B$, the minimum is attained only at $\pm(1,0), \pm(0,1)$ and $\pm(1,1)$.

Proof. See Theorem 2 of [2]. □

This leads to the following algorithm.
Input: Integers $b, c, d, a, c^2 - 4bd < 0, a > 0, gcd(b,c,d) = 1 = gcd(b,a)$.
Output: Solutions, if any, of $bt^2 + ctu + du^2 = a$ with $\gcd(t,u) = 1$.
Solve $b\theta^2 + c\theta + d \equiv 0 \pmod{a}, -a/2 < \theta \leq a/2$;
if there are no solutions, **exit**.
Let $\theta_0, \ldots, \theta_{s-1}$ be the solutions in the range $(-a/2, a/2]$;
$D := c^2 - 4bd$.
for $k = 0, \ldots, s-1$, $P := (b\theta_k^2 + c\theta_k + d)/a, Q := 2b\theta_k + c, R := ab$;
  calculate $\alpha, \beta, \gamma, \delta$, with $\alpha\delta - \beta\gamma = 1$ such that the transformation $u = \alpha X + \beta Y, y = \gamma X - \delta Y$ converts (p,q,r) to reduced form (A,B,C);
  if $A > 1$, **continue** to next k;
  if $A = 1$:
    if $C > 1$, $(u,y) := \pm(\alpha,\gamma)$;
    if $C = 1$ **and** $B = 0, (u,y) := \pm(\alpha,\gamma), \pm(\beta,\delta)$;
    if $C = 1$ **and** $B = 1$, $(u,y) := \pm(\alpha,\gamma), \pm(\beta,\delta), \pm(\alpha-\beta, -\gamma+\delta)$;
    print solutions $(t,u) := (\theta_k u - ay, u)$;
    continue to next k;
end for loop.

Remark. If $\gcd(b,a) > 1$, there exists a unimodular transformation of $bt^2 + ctu + du^2$ in which the first coefficient is now relatively prime to a. See [1, p. 286] for references.

Example. (Lagrange, [3, pp. 725–726]) Solve $t^2 + 7u^2 = 109, \gcd(t,u) = 1$. The solutions of $\theta^2 + 7 \equiv 0 \pmod{109}$ in the range $-109/2 < \theta \leq 109/2$ are $\theta = 50, -50$.

$\theta = 50$: The transformation $t = 50u - 109y$ converts $t^2 + 7u^2 = 109$ to $23u^2 - 100uy + 109y^2 = 1$.

The unimodular transformation $u = 2X - 9Y, y = X - 4Y$ converts $23u^2 - 100uy + 109y^2$ into the reduced form $X^2 + 7Y^2$. Its minimum is attained at $(X, Y) = \pm(1, 0)$, giving $(u, y) = \pm(2, 1)$ and $(t, u) = \pm(-9, 2)$.

Similarly $\theta = -50$ will give solutions $(t, u) = \pm(9, 2)$.

References

[1] K. R. Matthews, *The Diophantine equation* $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$. J. de Théorie des Nombres de Bordeaux **14** (2002) 257–270.

[2] Planet Math, *Reduced integral binary quadratic forms*, `http://planetmath.org/ReducedIntegralBinaryQuadraticForms`.

[3] J. A. Serret (Ed), *Oeuvres de Lagrange*, Gauthiers–Villars, 1877, `https://archive.org/details/uvresdelagrange02lagr`.