August 11, 2015

Consider the diophantine equation

$$ax^2 - by^2 = c, \tag{1}$$

where $\gcd(a,b) = 1, a > 0, b > 0, c \neq 0$ and ab is not a perfect square.

The LMM method generalizes to solve this equation if $\gcd(a,c) = 1$. See `http://www.numbertheory.org/pdfs/AX2-BY2=N.pdf`

But if $\gcd(a,c) > 1$, we can proceed as follows, along the lines of the treatment in [1].

Equation (1) becomes

$$X^2 - DY^2 = N, \tag{2}$$

where X=ax, Y=y, D=ab, N=ac.

Let (X,Y) be a fundamental solution for (2) and (t,u) be the fundamental solution for Pell's equation $u^2 - Dv^2 = 1$. Then a class of solutions (X_n, Y_n) of (2) is given by

$$X_n + Y_n\sqrt{D} = \pm(X + Y\sqrt{D})(t + u\sqrt{D})^n, n \in \mathbb{Z}. \tag{3}$$

Then (X_n, Y_n) gives an integer solution to (1) if and only if $X_n \equiv 0 \pmod{a}$.

Let $T_n + U_n\sqrt{D} = (t + u\sqrt{D})^n$. Then (3) gives

$$X_n = \pm(XT_n + DYU_n),$$
$$X_n \equiv \pm XT_n \pmod{a} \tag{4}$$

Now $T_n \equiv t^n \pmod{a}$; moreover $\gcd(t,a) = 1$, as $t^2 - abu^2 = 1$. So from (4), $X_n \equiv 0 \pmod{a}$ if and only if $X \equiv 0 \pmod{a}$. Hence if $X \equiv 0 \pmod{a}$ fails to hold, there is no resulting solution to (1). However if $X \equiv 0 \pmod{a}$ holds, then (3) yields a solution of (1) for all n.

An example. Solve $18x^2 - 5y^2 = 27$. Here $t = 19, u = 2$. The transformation $X = 18x, Y = y$ gives $X^2 - 90Y^2 = 486$. This has fundamental solutions $(X,Y) = (\pm 24, 1), (\pm 36, 3)$. Only the second gives solutions of $18x^2 - 5y^2 = 27$:

$$x = \pm(36/18)F + (270/18)G = \pm 2F + 15G,$$
$$y = 3F \pm 36G,$$

where $F + G\sqrt{90} = \pm(19 + 2\sqrt{90})^n, n \in \mathbb{Z}$.

References

[1] R.E. Sawilla, A.K. Silvester, H.C. Williams, *A new look at an old equation*, LNCS 5011, 37-59, 2008, especially pages 38-40.