Lagrange's Algorithm Strikes Again

How to write a prime as a sum of two squares

Benne de Weger
Eindhoven University of Technology
b.m.m.d.weger@tue.nl

version 1.0, July 7, 2012

Introduction. Wagon [W] gives an efficient elementary algorithm to find, for a given prime $p \equiv 1 \pmod 4$, integers x, y such that $p = x^2 + y^2$. It is based on the Euclidean Algorithm [E]. Actually, Wagon explains it in terms of a palindromic continued fraction. In this short note I rephrase this algorithm into what seems to be the modern language of Lattice Basis Reduction, but is just classical number theory due to Lagrange and Minkowski. To my taste, this simplifies the algorithm and its proof of correctness considerably.

Lattices. Consider the set

$$\Lambda_p = \left\{ (x,y) \in \mathbb{Z}^2 \,\middle|\, p | x^2 + y^2 \right\}.$$

See Fig. 1 for an example. There clearly is a lot of symmetry in this set: with (x,y) also $(-x,y), (x,-y)$ and (y,x) are in there. Maybe the structure of the set is not immediately clear from the picture. But staring at it for a few seconds, one might see that the points can be colored red and blue to reveal structure as shown in Fig. 2: Λ_p is the union of two orthogonal lattices. Indeed, let a be the integer between 0 and $\frac{1}{2}p$ such that $a^2 \equiv -1 \pmod p$. We introduce the sets

$$\Lambda_p^{\pm} = \left\{ (x,y) \in \mathbb{Z}^2 \,\middle|\, x \equiv \pm ay \pmod p \right\}.$$

Both these sets are lattices, with bases $\{(p,0), (\pm a, 1)\}$. We show that

$$\Lambda_p = \Lambda_p^+ \cup \Lambda_p^-.$$

Namely, $(x,y) \in \Lambda_p$ if and only if $x^2 + y^2 \equiv 0 \pmod p$, if and only if $(x,y) \equiv (0,0) \pmod p$ or $\left(xy^{-1}\right)^2 \equiv -1 \pmod p$, if and only if $(x,y) \equiv (0,0) \pmod p$ or $xy^{-1} \equiv \pm a \pmod p$, if and only if $x \equiv \pm ay \pmod p$, if and only if $(x,y) \in \Lambda_p^+ \cup \Lambda_p^-$. Note that the two lattices are each other's reflection in one of the axes. Also note that each of the two lattices is orthogonal, because whenever (x,y) is in $\Lambda_p^{\pm}$, then so is $(y,-x)$.

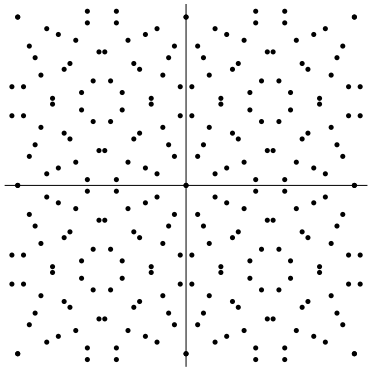

Fig. 1: The set Λ_{29}.

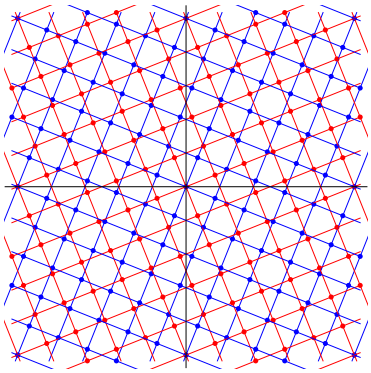

Fig. 2: Lattices in Λ_{29}.

Jacobi. As noted in [W], to find a such that $a^2 \equiv -1 \pmod{p}$, the following strategy works well in practice: try the successive primes $g = 2, 3, 5, \ldots$ until a quadratic nonresidue (mod p) is found, using the Jacobi symbol algorithm [J]; then take $a \equiv \pm g^{(p-1)/4} \pmod{p}$. On average one expects only two tries to be necessary. Unfortunately, good upper bounds on the minimally required number of tries are not known.

Minkowski. To prove the existence of x, y such that $x^2 + y^2 = p$, we invoke Minkowski's Convex Body Theorem [M]. It tells us that a disk centered at the origin contains a nonzero lattice point when its volume exceeds 4 times the volume of the lattice. If we denote the radius of the disk by r, then its volume is πr^2, and the volumes of our lattices equal p. It follows that we should take $r > \dfrac{2}{\sqrt{\pi}}\sqrt{p}$, to guarantee the existence of a point $(x, y) \in \Lambda_p$ with $0 < x^2 + y^2 < r^2$. Because $\pi > 2$, we can clearly take $r < \sqrt{2}\sqrt{p}$, so that $0 < x^2 + y^2 < 2p$. Because $(x, y) \in \Lambda_p$ it satisfies $p | x^2 + y^2$, and it follows that $x^2 + y^2$ must be equal to p.

Lagrange. It remains to argue that this line of reasoning gives not only existence of such an (x, y), but even an efficient algorithm to find it. Indeed, Lagrange's Algorithm[1] [L] does exactly this: given a basis of a 2-dimensional lattice, it finds a reduced basis of the lattice, in the sense that the lengths of the basis vectors are just the successive minima of the lattice. The algorithm simply works as follows: the basis $\{b_1, b_2\}$, assumed to satisfy $|b_1| \geq |b_2|$, is replaced by $\{b_2, b_1 - k b_2\}$, with $k \in \mathbb{Z}$ chosen such that $|b_1 - k b_2|$ is minimal, and this procedure is repeated as long as the basis improves. In our case, because of the orthogonality of the lattice, the reduced basis is $\{(x, y), \pm(y, -x)\}$, and the two successive minima are equal.

Example. We illustrate the algorithm with the example from [W]. Let $p = 73$. Then $g = 5$ is the smallest quadratic nonresidue, and $a \equiv 5^{18} \equiv 27 \pmod{73}$. The sequence of bases generated by Lagrange's algorithm is $\{(73, 0), (27, 1)\}$, $[k = 3]$: $\{(27, 1), (-8, -3)\}$, $[k = -3]$: $\{(-8, -3), (3, -8)\}$, [stop], and indeed $8^2 + 3^2 = 73$.

Performance. Heuristically the complexity of the algorithm equals the complexity of modular exponentiation, being almost quadratic in the size of the input, because Lagrange's algorithm has lower complexity. To illustrate the practical efficiency of the algorithm, I wrote a small Mathematica program, which took typically up to 20 seconds to generate a 1000 digit prime $\equiv 1 \pmod{4}$, and less than 0.1 second to find the corresponding x, y.

References

[E] Euclid, *Elements, Book VII, Book X*, Alexandria, approx. 300 BC.

[J] C.G.J. Jacobi, "Über die Kreisteilung und ihre Anwendung auf die Zahlentheorie", *Bericht Ak. Wiss. Berlin* [1837], pp. 127–136.

[L] J.L. Lagrange, "Recherches d'arithmétiques", *Nouv. Mém. Acad. Berlin*, 1773.

[M] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896.

[W] S. Wagon, "Editor's Corner: The Euclidean Algorithm Strikes Again", *Am. Math. Monthly* **97** [1990], 125–129.

[1] Lagrange's Algorithm is often attributed to Gauss, and in modern language it can be described as "2-dimensional lattice basis reduction". But essentially it is just the Euclidean Algorithm [E].