Liet. matem. rink., **44**, *spec. nr.*, 2004, 120–124

Factoring with Pell conics

Rasa ŠLEŽEVIČIENĖ (ŠU)
e-mail: rasa.slezeviciene@fm.su.lt

Abstract. In the paper the Pell conics method for factoring integers, based on observations of Lemmermeyer [2, 3], is presented explicitly. Moreover, a similar algorithm for factoring polynomials over finite fields is given.

Keywords: factoring, Pell conics.

1. Introduction

Factoring integers is a difficult task. Many cryptosystems in practise rely on the lack of having a fast (polynomial time) algorithm for factoring a given large integer. One of the most important (subexponential) algorithms is the elliptic curve factoring method of Lenstra [4]. In this brief note we present its relative for conics. The idea for such a factoring algorithm was proposed by Lemmermeyer [2,3]. Observing analogies between elliptic curves and conics, Lemmermeyer obtained (among other interesting similarities) a primality test based on Pell conics in the spirit of Lucas' classical test; in particular, a special choice of the underlying conic gives the well-known Lucas-Lehmer test for Mersenne numbers. Further, Lemmermeyer remarked the possibility to replace elliptic curves by conics in Lenstra's factoring algorithm; in [2] he gave an analogous algorithm in the related case of circles but he did not work out the details for Pell conics. It is the aim of this brief note to give such a factoring method explicitly. Furthermore, we treat the related problem of factoring polynomials over finite fields. Our approach cannot compete with well-known methods but might be interesting with regard to its simplicity.

2. Pell conics

Let $d \neq 1$ be a squarefree integer and put

$$\Delta = \begin{cases} d & \text{if} \quad d \equiv 1 \bmod 4, \\ 4d & \text{if} \quad d \equiv 2, 3 \bmod 4. \end{cases}$$

The affine curve of genus zero defined by the equation

$$\mathcal{X}^2 - \Delta \mathcal{Y}^2 = 4 \tag{1}$$

is called Pell conic, and we shall denote it by $\mathsf{C}(R)$ according to the ring R over which (1) is studied. Pell conics are irreducible, non-singular curves with a distinguished integral point $(2, 0)$. The quadratic diophantine equation (1) is a type of Pell equation

(after the English mathematician Pell who had nothing to do with it) and has been studied for more than two millenia; another form will be given below. Its set of solutions forms the group of units $\mu_{\mathbb{K}}$ in the quadratic number field $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta})$ with norm one. In fact, the mapping

$$\mathsf{C}(\mathbb{Z}) \ni (x, y) \mapsto \frac{1}{2}(x + y\sqrt{d}) \in \mu_{\mathbb{K}}$$

provides a group homomorphism.

If the underlying ring R is a field F, one can define a group law for the Pell conic $\mathsf{C}(F)$ as follows. Given two rational points $\mathcal{P}_1, \mathcal{P}_2 \in \mathsf{C}(F)$, take the line through $(2, 0)$ parallel to the line passing through $\mathcal{P}_1$ and $\mathcal{P}_2$. This line has a second point of intersection with the conic $\mathsf{C}(F)$ which we denote by $\mathcal{P}_1 + \mathcal{P}_2$. It is not too difficult to verify that this addition makes $\mathsf{C}(F)$ to an additive group with neutral element $(2, 0)$. Moreover, one can compute explicitly the coordinates of the sum of two points by the formula

$$(x_1, y_1) + (x_2, y_2) = \frac{1}{2}(x_1x_2 + y_1y_2\Delta, x_1y_2 + x_2y_1). \tag{2}$$

If $F = \mathbb{F}_q$ is a finite field with $q = p^d$ elements, then

$$\mathsf{C}(\mathbb{F}_q) = \mathbb{Z}/m\mathbb{Z}\,, \quad \text{where } m = q - \left(\frac{\Delta}{p}\right)^d, \tag{3}$$

and $(\frac{-}{p})$ denotes the Legendre symbol modulo p.

For more details we refer to [1] and [3].

3. Factoring integers

We want to find the factorization of a given composite integer N. The ring $\mathbb{Z}/N\mathbb{Z}$ is not a field, nevertheless, we shall consider Pell conics over $\mathbb{Z}/N\mathbb{Z}$. Since $\mathbb{Z}/N\mathbb{Z}$ is not a field, the conic $\mathsf{C}(\mathbb{Z}/N\mathbb{Z})$ splits into a proper product of residue class rings (different to (3)), each of these factors having order less than the group order. Now suppose that we know a point $\mathcal{P}$ on $\mathsf{C}(\mathbb{Z}/N\mathbb{Z})$ different from the neutral element $(2, 0)$. Further, assume that we already know a prime divisor p of N. Since the order of any element in $\mathsf{C}(\mathbb{Z}/p\mathbb{Z})$ divides the group order

$$c := \sharp\mathsf{C}(\mathbb{Z}/p\mathbb{Z}) = p - \left(\frac{\Delta}{p}\right)$$

of $\mathsf{C}(\mathbb{Z}/p\mathbb{Z})$, we have $c\mathcal{P} = (x, y)$ with

$$x \equiv 2 \text{ and } y \equiv 0 \mod p.$$

Thus, if N does not divide y, we may find a non-trivial divisor of N by computing $\gcd(x - 2, N)$ and $\gcd(y, N)$. This observation leads to a factoring algorithm. For this aim we notice that we can also work with any multiple of c. If c splits into *small* prime divisors ℓ, it is quite easy to find such a multiple. An integer is called B-smooth if all

of its prime divisors are less than or equal to B. If the group order c is B-smooth, the chances are good that $B!$ is a multiple of c.

We sum up all these observations in the following algorithm for factoring a given integer N.

1. Check with a standard primality test whether N is a prime power or not. If N is a prime power p^f, then RETURN p.

2. Choose a positive squarefree integer d and a point $\mathcal{P} \neq (2, 0)$ on the associated Pell conic C given by

$$\mathcal{X}^2 - \Delta \mathcal{Y}^2 \equiv 4 \bmod N.$$

3. Choose a positive integer B and compute $(B!)\mathcal{P} = (x, y)$ on C.

4. If N does not divide y RETURN $\gcd(x - 2, N)$ and $\gcd(y, N)$, otherwise increase B or choose a new random conic C with a point $\mathcal{P}$ and go back to Step 3.

From an algorithmical point of view it is reasonable to run this method parallel with several Pell conics. The multiplication $(B!)\mathcal{P}$ is performed by the standard use of fast exponentiation, that is representing $B!$ dyadically and adding the associated points $2^k\mathcal{P}$. Suitable points on a Pell conic can be found allong the lines of the solution of the associated Pell equation,

$$X^2 - dY^2 = 1, \tag{4}$$

by the continued fraction expansion of $\sqrt{\Delta}$.

We illustrate this method now with a very simple example, say $N = 35$. We know from the theory of the Pell equation that (2, 1) is a solution of (4) for $d = 3$. This gives us the point $\mathcal{P} = (4, 1)$ on the Pell conic $\mathrm{C}(\mathbb{Z}/35\mathbb{Z})$ with $\Delta = 12$. We may choose $B = 3$ and compute by (2)

$$2(4, 1) = (14, 4) \text{ and } 4(4, 1) = 2(14, 4) = (10, 28).$$

This leads to

$$(3!)\mathcal{P} = 2(4, 1) + 4(4, 1) = (14, 4) + (10, 28) = (7, 6),$$

which yields the factor $5 = 7 - 2$ of $N = 35$. Thus we arrive at $N = 35 = 5 \cdot 7$. Note that $\sharp\mathrm{C}(\mathbb{Z}/5\mathbb{Z}) = 6 = 2 \cdot 3$ (by (3) which corresponds to our choice of $B = 3$).

Recall Pollard's $p - 1$ method. By Fermat's little theorem we know that $2^{p-1} \equiv 1 \bmod p$ for any odd prime p. If $p - 1$ divides b, then $2^b \equiv 1 \bmod p$. So if p is a prime factor of N, then p divides $\gcd(2^b - 1, N)$. Pollard's method relies on the idea of factoring N by taking b having many divisors of the form $p - 1$. This is also the basis for Lenstra's celebrated elliptic curve factoring method [4]. However, compared with classical methods that worked with the multiplicative group modulo N, the use of elliptic curves has the advantage that there are lots of elliptic curves modulo a given number N. The same holds for Pell conics too. For further reading we refer to [5].

4. Factoring polynomials over finite fields

The same idea can be applied for factoring polynomials over finite fields. We restrict our investigations to the case of finite fields of the form $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, where p is prime. If P is an irreducible polynomial, then

$$\mathbb{F}_p[X]/P(X) = \{F(X) + P(X)\mathbb{F}_p[X]\colon\ F \in \mathbb{F}_p[X]\}$$

is a finite field of order p^d, where d is the degree of P, and so it is isomorphic to $\mathbb{F}_{p^d}$. Thus it makes sense to study Pell conics defined over such fields. They still obey a group law, and the order of this group is given by (3). We only have to take into account that the points on such conics have polynomial coordinates.

Now let $Q \in \mathbb{F}_p[X]$ be a reducible polynomial with irreducible divisor P of degree d. Suppose again that we know a point $\mathcal{P}$ on $\mathsf{C}(\mathbb{F}_p[X]/Q(X))$ different from the neutral element $(2, 0)$. By the same reasoning as in the previous section the order of any element in $\mathsf{C}(\mathbb{F}_p[X]/P(X))$ divides the group order

$$c = \sharp\mathsf{C}\big(\mathbb{F}_p[X]/P(X)\big) = p^d - \left(\frac{\Delta}{p}\right)^d,$$

and so we get $c\mathcal{P} = (x, y)$ with

$$x \equiv 2 \ \text{ and } \ y \equiv 0 \mod p.$$

Thus, if Q does not divide y, we get a non-trivial divisor of Q by computing $\gcd(x - 2, Q)$ and $\gcd(y, Q)$. The corresponding algorithm is

1. Check with a standard primality test whether Q is a irreducible or not. If Q is a power P^f of a reducible polynomial P, RETURN P.
2. Choose a positive squarefree integer d and a point $\mathcal{P} \neq (2, 0)$ on the associated Pell conic C given by
$$\mathcal{X}^2 - \Delta\mathcal{Y}^2 \equiv 4 \mod Q.$$
3. Choose a positive integer B and compute $(B!)\mathcal{P} = (x, y)$ on C.
4. If Q does not divide y RETURN $\gcd(x - 2, Q)$ and $\gcd(y, Q)$, otherwise increase B or choose a new random conic C with a point $\mathcal{P}$ and go back to Step 3.

We illustrate the algorithm by giving an example. We want to factor the polynomial $Q(X) = X^3 + X + 3$ over $\mathbb{F}_7$. We start with the point

$$\mathcal{P} = (X^2 + 3, 6X + 1)$$

on the conic defined by (1) with $\Delta = 5$ over $\mathbb{F}_7[X]/Q(X)$; note that we may reduce modulo Q, i.e., $X^3 = 6X + 4$. We compute

$$2\mathcal{P} = (5X^2 + 4X, X^2 + 5X + 6)$$

and find

$$\gcd\big(5X^2 + 4X + 5, Q(X)\big) = X + 2,$$

which yields the desired factorization of Q in $\mathbb{F}_7[X]$:

$$Q(X) = (X+2)(X^2+5X+5).$$

References

1. E.J. Barbeau, *Pell's Equation*, Springer (2003).
2. F. Lemmermeyer, Kreise und Quadrate modulo p, *Math. Semesterberichte*, **47**, 51–73 (2000).
3. F. Lemmermeyer, *Conics – a Poor Man's Elliptic Curves*, preprint, arXiv:math.NT/0311306 v1.
4. H.W. Lenstra, Factoring integers with elliptic curves, *Ann. of Math.*, **126**, 649–673 (1987).
5. L.C. Washington, *Elliptic Curves*, Chapman & Hall/CRC Press (2003).

REZIUMĖ

R. Šleževičienė. Faktorizavimas naudojant Pelio konikes

Straipsnyje išplėtojamos Lemmermeyer'io idėjos [2, 3] ir aprašomas sveikųjų skaičių faktorizavimo metodas naudojant Pelio konikes. Be to, pateikiamas panašus algoritmas polinomams virš baigtinių kūnų faktorizuoti.