university of groningen / faculty of science and engineering

University of Groningen

Bachelor Project Mathematics
11/07/2020

Integer Factorisation using Conics

Primary Supervisor:
Steffen Müller

Author:
D.S.L. Eelkema

Secondary Supervisor:
Pınar Kılıçer

Abstract

This thesis looks into factoring integers into their respective prime factorisation using conics. Inspired by Lenstra's Elliptic curve method, a factorisation algorithm is constructed based on the group law on Pell conics. It is found that this factorisation algorithm is actually a geometric representation of Williams' $p+1$ method. Using the fact that we have rediscovered Williams' $p+1$ method, a new proof for a theorem from Lehmer is also presented.

Contents

1 Introduction

This bachelor thesis looks into the construction of a integer factorisation algorithm, based on conics defined over a commutative ring. Factorisation algorithms have seen a resurgence in importance for numerous application such as RSA. RSA (see [10]) is a public-key encryption algorithm that is used to safely transfer data over a network. The algorithm relies on the difficulty of factorising the product of large prime numbers, more on this in section 2. Due to this, more research has gone into factorisation algorithms.

There are however already a lot of methods that are commonly used to factorise integers. Think of *Pollard's Rho algorithm*, *Pollard's* $p-1$ *method* (see [9]) or *Williams'* $p+1$ *method* (see [14]), just to name a few. There is also (see *Lenstra's elliptic curve method*). This method defines an elliptic curve over the commutative ring $\mathbb{Z}/N\mathbb{Z}$ with appropriate group law to reach a factorisation algorithm. Lemmermeyer shows in his Paper "A Poor man's elliptic curves" (see [5]) that a similar group law exists for Pell conics using geometry. By investigating the geometric structure of this group based on Pell conics, he finds similarities when comparing it to elliptic curves in his paper. Combining his unpublished notes (see [6]) with this paper, it becomes clear that a method can be constructed using Pell conics by means of a similar approach. That is what this thesis looks into.

The term Pell conic, comes from the term Pell's equation which is given as $x^2 - my^2 = 1$ for some integer m. The name of this equation came to be as the mathematician Euler, wrongly attributed the findings of Lord Brouncker's solution of the equation to a mathematician named John Pell. Already in 400 BC, mathematicians in Greece studied the properties and points on the Pell conic $x^2 - 2y^2 = 1$. Afterwards in 628 AC a scholar named Brahmagupta did pioneering work in finding solutions for the Pell equation $x^2 - 92y^2 = 1$

In the thesis we initially describe conics and a group law on conics is constructed. Then some examples of conics are given, eventually zooming in on Pell conics. The group order of a arbitrary Pell conic defined over the commutative ring $\mathbb{Z}/N\mathbb{Z}$ is also determined. From this group a condition can be found for when a point contains a factor of the integer we would like to factor.

The end goal is to construct a factorisation algorithm in *Sage* that can competitively factorise integers. For this, fast addition algorithms will be needed to speed up the computation time. Hence this thesis also looks into these methods.

2 Integer Factorisation

The problem of factorising integer is indeed a well defined problem since $\mathbb{Z}$ is a unique factorisation domain:

Definition 2.1. *A unique factorisation domain is a domain R in which for each element $a \in R$, $a \neq 0$ can be written uniquely as a product of a unit and a finite number of irreducible elements:*

$$a = u \cdot s_1 \cdot s_2 \cdot ... \cdot s_n, u \in R^\times, s_i \in R \text{ irreducible for } i \in 1, 2, ..., n$$

In the case of the ring $\mathbb{Z}$, the units are -1,1 and the irreducible elements are the prime numbers. Hence any integer can uniquely be written as a product of prime numbers multiplied with either 1 or -1. The question remains as to how integers can be factorised.

This knowledge is important as the prevalent encryption algorithm RSA relies on the difficulty of doing so. To illustrate how the encryption works, suppose person A would like to send the message M to person B over a public network. person B first comes up with two distinct, large, prime numbers p, q that are only known to him or her. The product $n = pq$ is publicly shared combined with an integer k. Person A can then encrypt the message M using the equation:

$$M^k \equiv c \bmod n$$

The encrypted message c is then made publicly available again to be decoded by person B. person B can decrypt the message by calculating the multiplicative inverse of k in $\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$:

$$ek \equiv 1 \bmod (p-1)(q-1),$$

because then $c^e \equiv M \mod n$. Of course this can only be done if p, q are known. The encryption relies on the fact that for outsiders, who don't know p and q, it is difficult to factorise n into p and q for large, complex prime numbers.

There are numerous methods that can do this efficiently, each with their own advantage based on the integer to be factored (see [1] for an overview of factorisation algorithms). Most important of those for this thesis are the so called Algebraic-group factorisation algorithms. These methods utilize the structure of groups to factorise integers. Among these are for example Pollard's $p-1$ algorithm and William's $p+1$ method. A short description of these two methods will shortly be presented. There is also Lenstra's elliptic curve method which defines an elliptic curve over a commutative ring to find a non-trivial factor. Unfortunately this thesis will not be able to go further into this method.

2.1 Pollard's $p-1$ method

Suppose that N is the composite number we would like to factor. Pollard's algorithm works by using Fermat's little theorem:

Theorem 2.1 (Fermat's little theorem)**.** *Let N be a composite number and $p \in \mathbb{Z}_{>1}$ an integer such that $p \mid N$. Let $a \in \mathbb{Z}_{>1}$ be an integer coprime to N, i.e.* $\gcd(a, N) = 1$*. Then for any $k \in \mathbb{Z}_{>0}$:*

$$a^{k(p-1)} \equiv 1 \bmod p$$

Let a be a coprime integer to N. The algorithm computes powers of this point a, $a^n, n \in \mathbb{Z}_{>1}$. Then $gcd(a^n - 1, N)$ is computed. If $(p-1) \mid n$ and $N \nmid n$, then this gcd will yield a non-trivial factor of N.

2.2 Williams' $p + 1$ Method

Williams' $p + 1$ method uses *Lucas Functions* to find a prime factor:

Definition 2.2 (Lucas Functions)**.** *For a quadratic polynomial $X^2 - Rx + 1$, $R \in \mathbb{Z}$, with roots $\alpha, \beta \in \mathbb{C}$, the Lucas functions are defined by:*

$$U_n(R) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z}$$
$$V_n(R) = \alpha^n + \beta^n \in \mathbb{Z}$$

In other literature the Lucas functions are based on quadratic polynomials of the form $X^2 - Rx + Q$, $Q \in \mathbb{Z}$. However, William proves in [14, section 3], that any Lucas Function can be reduced to one where the quadratic polynomial is of the form $X^2 - Rx + 1$. So for simplicity, this paper will solely focus on these. Later theorems can be proven exactly the same for a general $Q \in \mathbb{Z}$ although will take more effort. Now consider the following theorem:

Theorem 2.2 (Lehmer)**.** *Let p be an odd prime and $\left(\frac{\Delta}{p}\right) = \epsilon$, where $\Delta = R^2 - 4$, then:*

$$U_{(p-\epsilon)m}(R) \equiv 0 \ mod\ p$$
$$V_{(p-\epsilon)m}(R) \equiv 2 \ mod\ p$$

Proof. See Lehmer [4]. □

The proof in Williams' paper is quite dated and difficult to understand. Later a simpler proof based on Pell Conics will be given. This theorem gives a condition to find a non-trivial factor of an integer N using Lucas functions. Since if n is a multiple of $(p - \epsilon)$, and $N \nmid n$, then $\gcd(V_n(R) - 2, N)$ yields a non-trivial factor of N.

3 Conics

To construct a factorisation algorithm based on conics, one must first be familiar with the notion of a conic over a ring. Conics are plane algebraic curves defined by a polynomial of degree 2.

Definition 3.1 (Conic)**.** *Let $a, b, ..., f \in R$, R a commutative ring, such that at least a, b or c is non-zero. The equation $ax^2 + by^2 + cxy + dx + ey + f = 0$ defines a conic C. We write C over R.*

We define the set of R-rational points on a conic C to be:

Definition 3.2. *Let R be a commutative ring. The set of R-rational points on a conic $C : ax^2 + by^2 + cxy + dx + ey + f = 0$ over R is denoted by:*

$$C(R) := \{(x, y) \in R \times R \mid ax^2 + by^2 + cxy + dx + ey + f = 0\}$$

Now let R be a field, and let C over R be a conic. We now construct a geometric abelian group law on $C(R)$. We will later give explicit formulas for this group law on specific conics. These formulas will show that there is in fact an abelian group law on $C(R)$ for arbitrary commutative rings.

Definition 3.3 (The group law on conics)**.** *Let $P, Q \in C(R)$ and fix some $e \in C(R)$ to be (can be any element in $C(R)$) the unit element. The sum of P and Q is defined as follows:*

We draw a line between P and Q, say PQ. Then we draw a line parallel to PQ that intersects with our unit element e, call it $l(P+Q)$. This line $l(P+Q)$ intersects with our conic in at most two points. Indeed, intersecting a line with a curve defined by a second degree polynomial yields two intersections at most. If there is any other intersection than e, then this will be the sum of $P + Q$. Else $P + Q = e$. If we take $P = Q$ then the line PQ will simply be the tangent at the point P.

To show that this group law is properly defined, we must go through the axioms of what defines a group. First we need to show that $P + Q \in C(R)$. To do this, first note that for $P, Q \in C(R)$, the line $l(P + Q)$ trough e has coefficients in R. One can construct this line simply enough by writing $P = (x_1, y_1), Q = (x_2, y_2), e = (e_1, e_2)$. Then if $x_1 \neq x_2$:

$$y = mx + g, \text{ where } m = \frac{y_1 - y_2}{x_1 - x_2} \text{ and } g = e_2 - me_1$$

Since R is a field, naturally $b, m \in R$ since they are the result of additions and multiplications of elements in R. In the case that $x_1 - x_2 = 0$, the line $l(P+Q)$ is simply the line $y = g$ intersecting e. Now the conic $C : ax^2 + by^2 + cxy + dx + ey + f = 0$ can be intersected with $l(P + Q)$: By construction (e_1, e_2) is an element of $C(R)$ and a point on the curve $y = mx + g$. Substituting for $y = mx + g$ on the conic C, we find a quadratic polynomial for which e_1 is a

zero. This polynomial can then be written as $(x - e_1)r(x), r(x) \in R[X]$. Since this polynomial has a zero in R, a field, then as this is a quadratic polynomial, the other zero is contained in R as well. Suppose this other zero is x^*. Then writing $y^* = mx^* + g \in R$, we have found the addition of P and Q, namely $P + Q = (x^*, y^*) \in C(R)$. Hence the addition is well defined.

Now the following theorem can be proven:

Theorem 3.1. *Let $C : ax^2 + by^2 + cxy + dx + ey + f = 0$ be a conic defined over a field R, $C(R)$. Let $e \in C(R)$. Then definition 3.3 defines an abelian group law on $C(R)$ with unit element e.*

The thesis mainly discusses Pell conics so only a sketch of the proof will be given below. Later the theorem will be explicitly proven for Pell conics, where this theorem will also extend to Commutative rings:

Proof. The theorem can be proven by considering the axioms for a abelian group.:

I. To show associativity is quite technical. For a proof of the associativity see [11, section 3]; utilising Pascal's Hexagon Theorem (see [12]) an easy proof can be constructed. Later we will prove it for the special case of a Pell conic.

II. Trivially for $P \in C(R)$, when wanting to compute $P + e$, simply note that $l(P + e)$ is equal to the line Pe. By construction, $P + e = e + P = P$

III. The inverse of a point $P \in C(R)$ can be computed as follows. Take the tangent of the unit element e. Now construct a line with the slope of this tangent intersecting P. Then P^{-1} is defined to be the other intersection this line makes with the conic. If there is no other intersection except for P, then $P^{-1} = P$. By construction $P + P^{-1} = e$.

IV. Commutativity is trivial because of the way this group law has been constructed. For $P, Q \in C(R)$. The slope between P and Q is the same as the slope between Q and P. Hence, $P + Q = Q + P$

□

Below some examples of Conics are presented.

3.1 The Parabola

To illustrate the group law on conics we take the conic $\mathcal{K} : y = x^2$ over the rational numbers $\mathbb{Q}$. This then defines the $\mathbb{Q}$-rational points $\mathcal{K}(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y = x^2\}$. Let the unit element be $(0, 0)$. Take the two points $P = (-1, 1), Q = (2, 4) \in \mathcal{K}(\mathbb{Q})$. The sum $P + Q = (1, 1)$ is illustrated below:

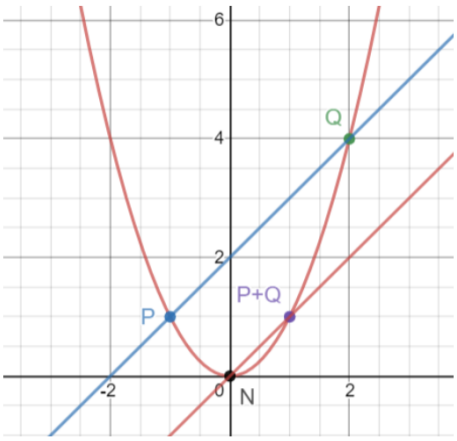

Figure 1: Sum of P and Q on the conic $x^2 = y$

This group law can also be written explicitly as:

Definition 3.4. *Let $P = (x_1, x_1^2), Q = (x_2, x_2^2) \in \mathcal{K}(R)$, and let the unit element be $(0, 0)$. The sum of P and Q is then defined as:*

$$(x_1, x_1^2) + (x_2, x_2^2) = (x_1 + x_2, (x_1 + x_2)^2)$$

This defines a group for any commutative ring R (see [6, section 2.2]), and is the same as definition 3.3 when R is a field.

3.2 The Hyperbola $\mathcal{H}$

The formula for a hyperbola is given by: $\mathcal{H} : xy = 1$. We can again define the R-rational points $\mathcal{H}(R) = \{(x, y) \in R \times R \mid xy = 1\}$. In this case let's compute the group law explicitly, when R is a field.

Let the unit element be $(1, 1) \in \mathcal{H}(R)$ where 1 is the unit element of R Take $(a, a^{-1}), (b, b^{-1}) \in \mathcal{H}(R)$. The slope m of the line between these points can then simply be computed by:

$$m = \frac{a^{-1} - b^{-1}}{a - b} = -\frac{1}{ab}$$

If $a = b$ then $(a, a^{-1}) = (b, b^{-1})$. Hence the slope m will just be tangent of the hyperbola at the point (a, a^{-1}). Now we find the parallel line by plugging in our unit element $(1, 1)$ into the equation $y = mx + C$ to find:

$$y = -\frac{1}{ab}x + C = -\frac{1}{ab}(x - 1) + 1$$

Then this line can be intersected with the hyperbola to obtain:

$$\left.\begin{array}{ll} y & = -\frac{1}{ab}(x-1)+1 \\ xy & = 1 \end{array}\right\} x - 1 = \frac{1}{ab}(x-1)x$$

So either $x = 1$, yielding the unit element, or $x = \frac{1}{ab}$. Thus we find:

Definition 3.5. *Let $(a, a^{-1}), (b, b^{-1}) \in \mathcal{H}(R)$ where $\mathcal{H}(R)$ has unit element $(1, 1)$ the sum of (a, a^{-1}) and (b, b^{-1}) is defined as:*

$$(a, a^{-1}) + (b, b^{-1}) = (ab, (ab)^{-1})$$

Holding on to our previous construction it's clear that this will define an abelian group $(\mathcal{H}(R), +, (1, 1))$ for any commutative ring R. For the inverse of an element $P = (a, a^{-1}) \in \mathcal{H}(R)$, following the construction described in section 3, we find: $P^{-1} = (a^{-1}, a)$. It is also clear that $P+(1, 1) = (1, 1)+P = P$. I will leave it as an exercise to the reader to completely show that this construction indeed defines a group. It is trivial to see that in fact all elements that satisfy the equation of the hyperbola over R correspond to a unique unit elements in R, $R^\times$ by definition. By definition 3.5:

$$\mathcal{H}(R) \simeq R^\times$$

To illustrate this group law, take the Hyperbola over the rational numbers $\mathbb{Q}$, $\mathcal{H}(\mathbb{Q})$. Let $P = \left(\frac{5}{9}, \frac{9}{5}\right), Q = \left(-\frac{4}{5}, -\frac{5}{4}\right)$ Then the sum $P + Q = \left(-\frac{4}{9}, -\frac{9}{4}\right)$:

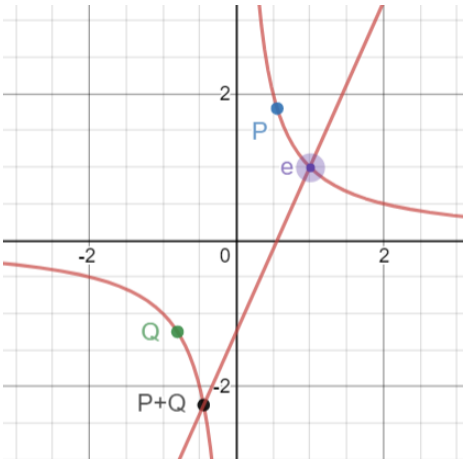

Figure 2: Sum of P and Q on the conic $xy = 1$

3.3 The Pell conic

Definition 3.6 (The Pell conic defined over R)**.** *Let R be a commutative ring. A Pell conic C_m over R is defined by an equation $x^2 - my^2 = 1$, where $m \in R$*

$$\textit{Hence, } C_m(R) = \{(x, y) \in R \times R \mid x^2 - my^2 = 1\},$$

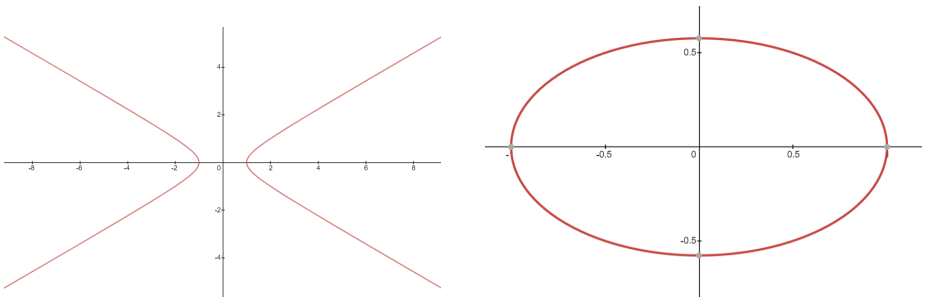

Figure 3: The Pell conics $x^2 - 3y^2 = 1$ and $x^2 + 3y^2 = 1$ respectively.

Let us go through the steps to find the group law on a Pell conic. To this end we let our unit element $e = (1, 0) \in C_m(R)$ where 1 and 0 are the unit and zero element of R respectively.

Definition 3.7. *For $(x_1, y_1), (x_2, y_2) \in C_m(R)$, the sum is defined to be:*

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + my_1y_2, x_1y_2 + x_2y_1)$$

Van der Sluis proved that in the case for $m = 3$, $(C_3(R), +, e)$, with addition $+$ as above, defines a group in [13]. Now we will prove the general case.

Theorem 3.2. *$(C_m(R), +, e)$ is a group.*

Proof. I. Indeed, for $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in C_m(R)$ we have:

$$\begin{aligned}((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) =& (x_1x_2 + my_1y_2, x_1y_2 + x_2y_1) + (x_3, y_3)\\ =& (x_1(x_2x_3 + my_2y_3) + my_1(x_3y_2 + y_3x_2),\\ & x_1(x_3y_2 + x_2y_3) + y_1(x_2x_3 + my_2y_3))\\ =& (x_1, y_1) + ((x_2, y_2) + (x_3, y_3))\end{aligned}$$

II. For $e = (1, 0)$ and $(x_1, y_1) \in C_m(R)$ we have:

$$e + (x_1, y_1) = (x_1, y_1) = (x_1, y_1) + e$$

III. For $P = (x_1, y_1) \in C_m(R)$ Let $P^{-1} = (x_1, -y_1)$. Then:

$$\begin{aligned}P + P^{-1} = (x_1, y_1) + (x_1, -y_1) &= (x_1^2 - my_1^2, 0)\\ &= (1, 0)\\ &= (x_1, -y_1) + (x_1, y_1)\end{aligned}$$

IV. Trivially for $(x_1, y_1), (x_2, y_2) \in C_m(R)$:

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + my_1y_2, x_1y_2 + x_2y_1) = (x_2, y_2) + (x_1, y_1)$$

, since R itself is commutative. Hence $(C_m(R), +, e)$ is a group. □

If R is a field, then this group law is the same as the group law constructed in Definition 3.3. To show this group law is the same, it can be checked that the slope $t = \frac{y_1-y_2}{x_1-x_2}$ is in fact the same slope as the slope obtained from the line intersecting $e = (1, 0)$ and $(x_1x_2 + my_1y_2, x_1y_2 + x_2y_1)$ which is $\frac{x_1x_2+my_1y_2}{x_1y_2+x_2y_1-1}$. Note that for checking

$$\frac{x_1x_2 + my_1y_2}{x_1y_2 + x_2y_1 - 1} = \frac{y_1 - y_2}{x_1 - x_2},$$

we can check the following:

$$\begin{aligned}
(x_1x_2 + my_1y_2)(x_1 - x_2) &= (y_1 - y_2)(x_1y_2 + x_2y_1 - 1) \\
x_1^2y_2 + x_1x_2y_1 - x_1x_2y_2 - x_2^2y_1 &= x_1x_2y_1 + my_1^2y_2 - y_1 - y_2x_1x_2 - my_1y_2 + y_2 \\
(x_1^2 - my_1^2 - 1)y_2 &= (x_2^2 - my_2^2 - 1)y_1 \\
0 &= 0
\end{aligned}$$

Hence the slopes are equal and therefore $(x_1x_2+my_1y_2, x_1y_2+x_2y_1)$ is the point we find by geometrically calculating the sum $(x_1, y_1) + (x_2, y_2)$.

3.3.1 Relation between $R[\alpha]$ and $C_m(R)$

Points on a Pell conics $C_m(R)$ are often studied as a subset of the ring $R[\alpha]$. As before, let R be a commutative ring and consider the polynomial ring:

$$S = R[x]/(x^2 - m)$$

Let $\alpha \in S$ such that $\alpha^2 = m$. Define:

$$R[\alpha] := \{x + y\alpha \mid x, y \in R\}$$

Proposition 3.1. *$(R[\alpha], +, \cdot, 0, 1)$ is a commutative ring with $0, 1 \in R$ and addition and multiplication rules:*

$$\begin{aligned}
(x_1 + y_1\alpha) + (x_2 + y_2\alpha) &= x_1 + x_2 + (y_1 + y_2)\alpha \\
(x_1 + y_1\alpha)(x_2 + y_2\alpha) &= x_1x_2 + my_1y_2 + (x_1y_2 + x_2y_1)\alpha
\end{aligned}$$

It is trivial to see that this indeed yields a ring. Let the norm map $\mathcal{N}$ over this ring be defined as:

$$\begin{aligned}
&\mathcal{N}: \ R[\alpha] \to R \\
&x + y\sqrt{m} \to (x + y\sqrt{m})(x - y\sqrt{m})
\end{aligned}$$

This map $\mathcal{N}$ is multiplicative; we have that for $(x_1 + y_1\alpha), (x_2 + y_2\alpha) \in R[\alpha]$:

$$\begin{aligned}\mathcal{N}((x_1 + y_1\alpha)(x_2 + y_2\alpha)) =& \mathcal{N}(x_1x_2 + my_1y_2 + (x_1y_2 + x_2y_1)\alpha) \\ =& (x_1x_2 + my_1y_2)^2 - m(x_1y_2 + x_2y_1)^2 \\ =& x_1^2x_2^2 - mx_1^2y_2^2 - mx_2^2y_1^2 + m^2y_1^2y_2^2 \\ =& (x_1^2 - my_1^2)(x_2^2 - my_2^2) \\ =& \mathcal{N}(x_1 + y_1\alpha)\mathcal{N}(x_2 + y_2\alpha)\end{aligned}$$

Hence the map $\mathcal{N}$ restricted to the units:

$$\mathcal{N} : \ R[\alpha]^\times \to R^\times,$$

is a group homomorphism and $\ker(\mathcal{N})$ is a subgroup of $R[\alpha]^\times$. Define $T_m(R) := \ker(\mathcal{N})$. We can now prove the following:

Theorem 3.3. *Let R be a commutative ring, and let $m \in R$. Then:*

$$T_m(R) \simeq C_m(R) \tag{1}$$

Proof. Consider the homomorphism:

$$\begin{aligned}\Theta : T_m(R) &\to C_m(R) \\ x + y\alpha &\to (x, y)\end{aligned}$$

This map is well defined since by definition $\mathcal{N}(x + y\sqrt{m}) = x^2 - my^2 = 1$, so $\Theta(x + y\sqrt{m}) = (x, y) \in C_m(R)$. Now to show Θ is a homomorphism, let $x_1 + y_1\sqrt{m}, x_2 + y_2\sqrt{m} \in T_m(R)$:

$$\begin{aligned}\Theta((x_1 + y_1\alpha)(x_2 + y_2\alpha)) &= \Theta(x_1x_2 + my_1y_2 + (x_1y_2 + x_2y_1)\alpha) \\ &= (x_1x_2 + my_1y_2, x_1y_2 + x_2y_1) \\ &= (x_1, y_1) + (x_2, y_2) \\ &= \Theta(x_1 + y_1\alpha) + \Theta(x_1 + y_2\alpha)\end{aligned}$$

So Θ is a homomorphism. Bijectivity is trivial, hence is therefore left as an exercise for the reader. Hence Θ is an Isomorphism.

□

The extension $R[\alpha]$ is equal to R if m is a square in R as then $\alpha \in R$. Hence $T_m(R) = R^\times$. This set $T_m(R)$ will however not be trivial if m is not a square.

4 Factorisation algorithms based on conics

The main focus of this thesis is to compute the prime factorisation of integers. So let N be a composite number, the integer we wish to factor. Two algorithms are discussed, one less interesting method based on the hyperbola $\mathcal{H}$, and one based on Pell conics C_m. As prerequisite we only need one elementary theorem from Group Theory, generalising Theorem 2.1:

Theorem 4.1. *Let G be a finite group with order $\#G = g$ and unit element e. Then for any element $x \in G$:*

$$x^g = e$$

For the algorithms to succeed, we restrict to integers N not divisible by 2. If N does contain factors of 2 we can simply divide N by 2 until that is no longer the case.

4.1 Rediscovering Pollard's $p-1$ method with $\mathcal{H}(R)$

Let N be the composite number to be factored. Take $\mathcal{H}$ as before but now with $R = \mathbb{Z}/N\mathbb{Z}$. Since $\mathbb{Z}/N\mathbb{Z}$ is a commutative ring this again defines an abelian group $(\mathcal{H}(\mathbb{Z}/N\mathbb{Z}), +, (1,1))$ with addition $+$ defined as before. For $n \in \mathbb{Z}_{>0}$ let nP denote a point $P \in \mathbb{Z}/N\mathbb{Z}$ added to itself n many times. Let $nP = (b, b^{-1})$, then $-nP = (b^{-1}, b)$.

Lemma 4.2. *Let $(a, a^{-1}) \in \mathcal{H}(\mathbb{Z}/N\mathbb{Z})$, $(a, a^{-1}) \neq (1,1)$. Suppose p is a prime divisor of N. Let k be a multiple of $p-1$ and $kP = (b, b^{-1})$ mod N for some $b \in \mathbb{Z}/N\mathbb{Z}$. Then:*

$$(b, b^{-1}) \equiv (1,1) \bmod p$$

Proof. Since $(a, a^{-1}) \in \mathcal{H}(\mathbb{Z}/N\mathbb{Z})$, $a \neq 1$ we have that a is coprime to N. But then a must also be coprime to p so $(a \bmod p, a^{-1} \bmod p) \in \mathcal{H}(\mathbb{Z}/p\mathbb{Z})$. Trivially $\#\mathcal{H}(\mathbb{Z}/p\mathbb{Z}) = p-1$ so by theorem (3.1), $(p-1)(a, a^{-1}) \equiv (1,1) \bmod p$. □

Note that in this case $b-1 \equiv 0 \bmod p$, meaning $p \mid b-1$. Combined with the fact that $p \mid N$ we have now found a condition for finding a non-trivial divisor. Namely:

Corollary 4.2.1. *Let $kP = (b, b^{-1})$ be as before where k is a multiple of $p-1$, $P \in \mathcal{H}(\mathbb{Z}/N\mathbb{Z})$ and p a non-trivial divisor of N. Then:*

$$\gcd(b-1, N) \text{ is a non-trivial divisor of } N \Leftrightarrow b-1 \not\equiv 0 \text{ mod } N$$

So to get a factorisation algorithm, one can simply take an integer a coprime to N and compute multiples, $a^n \bmod N$. Then $\gcd(a^n - 1, N)$ will most likely deliver a non-trivial divisor if $p \mid a^n - 1$, meaning that n is a multiple of $p-1$. Of course $p-1$ is unknown so an appropriate guess has to be made. In practice one can do no better than to guess $n = b!$, for some integer $b \in \mathbb{Z}_{>0}$. For big enough b there is a good chance that $p-1$ is a factor of n if $p-1$ is *smooth*. An integer is smooth if all its prime divisors are small.

4.1.1 Sketch of factorisation algorithm using $\mathcal{H}$

Below a sketch of the algorithm is presented based on the Hyperbola $\mathcal{H}$:

Data: Integer N
Result: Non-Trivial factor of N
$b = 2$;
$a = 2$ (integer such that $\gcd(a, N) = 1$);
$P = (a, a^{-1}) \in \mathcal{H}(\mathbb{Z}/N\mathbb{Z})$;
while *No non-trivial factor has been found* **do**
  compute $b!P = (a^{b!}, (a^{-1})^{b!})$;
  if $\gcd((b!P)_x - 1, N) \neq 1$ **then**
    if $\gcd((b!P)_x - 1, N) = N$ **then**
      print(multiple of N);
      Take a new P;
    else
      non-trivial factor has been found;
      print($\gcd((b!P)_x - 1, N)$)
    end
  else
    $b = b + 1$;
  end
end

Algorithm 1: To factorize an integer N

Trivially if $a^n = 1$ then $(a^{-1})^n = 1$ so we don't have to test for $(a^{-1})^n$ as well. Typically one takes $a = 2$, since it is easy to check whether N is divisible by 2 and earlier we assumed that $2 \nmid N$, but a can also be chosen differently. In fact this whole description is equivalent to Pollard's $p - 1$ method described in section 2.1 (see [9]). Hence a geometric description of Pollard's $p - 1$ method has been found.

4.2 Factorisation algorithm on Pell conics

Again, let N be the composite number to be factored, let $m \in \mathbb{Z}/N\mathbb{Z}$ and consider $C_m(\mathbb{Z}/N\mathbb{Z})$. A similar factorisation can be established using Pell conics:

Lemma 4.3. *Let p be a prime factor of N. Then there exists a group homomorphism between $C_m(\mathbb{Z}/N\mathbb{Z})$ and $C_m(\mathbb{Z}/p\mathbb{Z})$ namely:*

$$\begin{aligned} \phi : C_m(\mathbb{Z}/N\mathbb{Z}) &\to C_m(\mathbb{Z}/p\mathbb{Z}) \\ (x, y) &\to (x \bmod p, y \bmod p) \end{aligned}$$

Proof. To show this homomorphism is well defined let $(x, y) \in C_m(\mathbb{Z}/N\mathbb{Z})$. Then:

$$\begin{aligned} x^2 - my^2 &\equiv 1 \bmod N \\ &\equiv 1 \bmod p \end{aligned}$$

So $\phi((x,y)) = (x \bmod p, y \bmod p) \in C_m(\mathbb{Z}/p\mathbb{Z})$. Now let $(x_1,y_1),(x_2,y_2) \in C_m(\mathbb{Z}/N\mathbb{Z})$. Then:

$$\begin{aligned}\phi((x_1,y_1)+(x_2,y_2)) &= \phi((x_1x_2+my_1y_2, x_1y_2+x_2y_1)) \\ &= (x_1x_2+my_1y_2 \bmod p, x_1y_2+x_2y_1 \bmod p) \\ &= (x_1 \bmod p, y_1 \bmod p)+(x_2 \bmod p, y_2 \bmod p) \\ &= \phi((x_1,y_1))+\phi((x_2,y_2))\end{aligned}$$

Hence ϕ is a homomorphism between $C_m(\mathbb{Z}/N\mathbb{Z})$ and $C_m(\mathbb{Z}/p\mathbb{Z})$, proving the claim. □

So reducing points $P \in C_m(\mathbb{Z}/N\mathbb{Z})$ modulo p yields points on the Pell conic $C_m(\mathbb{Z}/p\mathbb{Z})$. Also adding a point on the $C_m(\mathbb{Z}/N\mathbb{Z})$ k many times and then taking the reduction map, is equivalent to first reducing the point and then adding it to itself k many times on $C_m(\mathbb{Z}/p\mathbb{Z})$. This will be useful for proving the following lemma.

Lemma 4.4. *Let $P \in C_m(\mathbb{Z}/N\mathbb{Z})$. Suppose that p is a prime factor of N and let $\#C_m(\mathbb{Z}/p\mathbb{Z}) = g$. Then take k to be some multiple of g. Let $kP = (x,y)$ where $x,y \in \mathbb{Z}/N\mathbb{Z}$. Then:*

$$(x,y) \equiv (1 \bmod p, 0 \bmod p)$$

Proof. Let $P = (x,y) \in C_m(\mathbb{Z}/N\mathbb{Z})$; then $(x \bmod p, y \bmod p) \in C_m(\mathbb{Z}/p\mathbb{Z})$ by lemma 4.3. Because $C_m(\mathbb{Z}/p\mathbb{Z})$ has finite order, this implies by theorem 4.1 that :

$$\phi(gP) = (1 \bmod p, 0 \bmod p)$$

where ϕ is the homomorphism defined in in Lemma 4.3. So also $\phi(kP) = (1 \bmod p, 0 \bmod p)$, proving the lemma. □

Hence, as long as the order of $C_m(\mathbb{Z}/p\mathbb{Z})$ is known we have a condition for finding a non-trivial divisor. Because when $(x,y) \equiv (1,0) \bmod p$ then as long as $x \not\equiv 1 \bmod N$ and/or $y \not\equiv 0 \bmod N$, taking the gcd with N yields a non-trivial divisor:

Corollary 4.4.1. *Let $P \in C_m(\mathbb{Z}/N\mathbb{Z})$, where N is the integer to be factored. Suppose that p is a prime factor of N and let $\#C_m(\mathbb{Z}/p\mathbb{Z}) = g$. Then take k to be some multiple of g. Also let $kP = (x,y)$ where $x,y \in \mathbb{Z}/N\mathbb{Z}$. Then:*

$$\begin{aligned}\gcd(x-1,N) \text{ is a non-trivial divisor of } N &\Leftrightarrow x \not\equiv 1 \bmod N \\ \gcd(y,N) \text{ is a non-trivial divisor of } N &\Leftrightarrow y \not\equiv 0 \bmod N\end{aligned}$$

So computing multiples of a point P on a Pell conic $C_m(\mathbb{Z}/N\mathbb{Z})$ gives a method for finding factors out of N. We can be almost sure that $x \not\equiv 1 \bmod N$ as long as a point P with high enough order in $C_m(\mathbb{Z}/N\mathbb{Z})$ is taken. If $x-1$ is

a multiple of N then either n is too big or the order of P is too small. Then one can first try to use factors of n and if that does not yield a non-trivial divisor then try a different point P.

Also note that computing $\gcd(y, N)$ is equivalent to computing $\gcd(x+1, N)$ and $\gcd(x-1, N)$. This is because if $y \equiv 0 \bmod p$, then $x^2 \equiv 1 \bmod p$, implying $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$. Alternatively to computing $\gcd(x+1, N)$, we can compute $\gcd(x'-1, N)$ where x' is the x-coordinate of $2nP$. This will be useful later when speeding up the algorithm. Now all that is left is to find this order $\#C_m(\mathbb{Z}/p\mathbb{Z})$

4.2.1 Finding the order of $C_m(\mathbb{Z}/p\mathbb{Z})$

To find the $\mathbb{Z}/p\mathbb{Z}$-rational points on the Pell conic C_m, a parameterisation is constructed. This can be done geometrically by intersecting a line with the Pell conic. Note that for any $m \in \mathbb{Z}$, we have that $P = (-1, 0) \in C_m(\mathbb{Z}/p\mathbb{Z})$. Let $p \nmid m$. Let $y = tx + b$ be a line intersecting this point P. Then $b = t$, which implies $y = t(x+1)$. Intersecting this line with the Pell conic yields:

$$x^2 - 1 - mt^2(x+1)^2 = 0$$

Clearly $x = -1$ is a solution so this can be rewritten to be:

$$(x+1)(x(1-mt^2) - 1 - mt^2) = 0$$

Hence a solution $x \neq 1$ must satisfy:

$$x(1-mt^2) = 1 + mt^2$$

This yields $x = \frac{1+mt^2}{1-mt^2}$ and therefore $y = \frac{2t}{1-mt^2}$. Hence the parameterisation is given by:

$$\begin{aligned} \mathbb{Z}/p\mathbb{Z} &\to C^m(\mathbb{Z}/p\mathbb{Z}) \\ t &\to \left(\frac{1+mt^2}{1-mt^2}, \frac{2t}{1-mt^2}\right) \end{aligned}$$

Of course this only works for values $t \in \mathbb{Z}/p\mathbb{Z}$ such that $1 - mt^2 \neq 0$. All p points in $\mathbb{Z}/p\mathbb{Z}$ give points on the Pell conic except if there is an element $t \in \mathbb{Z}/p\mathbb{Z}$ such that $t^2 = \frac{1}{m}$. If there is such an element then there are exactly two. Combined with the point $(-1, 0)$, the order of $C^m(\mathbb{Z}/p\mathbb{Z})$ will either be $p-1$ or $p+1$. This gives rise to the following theorem:

Theorem 4.5. *Suppose that $m \in \mathbb{Z}$, $p \nmid m$. Then:*

$$\#C_m(\mathbb{Z}/p\mathbb{Z}) = p - \left(\frac{m}{p}\right) = \begin{cases} p-1 \text{ if } t^2 \equiv m \mod p \text{ has a solution} \\ p+1 \text{ if } t^2 \equiv m \mod p \text{ has no solutions} \end{cases}$$

Here, $\left(\frac{m}{p}\right)$ stands for the Legendre Symbol.

Proof. Before we showed if $\frac{1}{m}$ is a square in $\mathbb{Z}/p\mathbb{Z}$, then the order of $C_m(\mathbb{Z}/p\mathbb{Z})$ is $p-1$ and $p+1$ if $\frac{1}{m}$ is not a square. But $\frac{1}{m}$ is a square, if and only if $\frac{1}{m}m^2 = m$ is also square. □

4.2.2 Sketch of a factorisation algorithm using C_m

From the previous theorem it becomes clear that the order of $C_m(\mathbb{Z}/p\mathbb{Z})$ is determined by whether $m \bmod p$ is a quadratic residue mod p in $\mathbb{Z}/p\mathbb{Z}$; in other words it is determined by the Legendre Symbol $\left(\frac{m}{p}\right)$. Let $\epsilon = \left(\frac{m}{p}\right)$. Suppose n is a multiple of $p - \epsilon$. Then $\gcd((nP)_x - 1, N)$ will likely result in a non-trivial factor of N, for $P \in C_m(\mathbb{Z}/N\mathbb{Z})$. If $\epsilon = 1$, then n needs to be such that $p-1 \mid n$. This is then however the same as the $p-1$ method; we take $n = b!$, for $b \in \mathbb{Z}_{>0}$ and hope that $p-1$ is smooth. Therefore applying this method when $\epsilon = 1$ yields the same factors of N as the $p-1$ would. Hence we prefer $\epsilon = -1$ because then we find factors p of N where $p+1$ is smooth. Of course it is not known whether or not m is a quadratic residue mod p before we know p. To increase the chances of $\epsilon = -1$, a random Pell conic C_m is taken. A sketch of the initial algorithm is given below:

Data: Integer N
Result: Non-Trivial factor of N
$b = 2$;
Take random $m \in (\mathbb{Z}/N\mathbb{Z}), m \neq 0$;
Take random $P \in C_m(\mathbb{Z}/N\mathbb{Z})$;
while *No non-trivial factor has been found* **do**
  compute $b!P = (x, y)$;
  if $\gcd((b!P)_x - 1, N) \neq 1$ **then**
    if $\gcd((b!P)_x - 1, N) = N$ **then**
      print(multiple of N);
      Take a new P;
    else
      non-trivial factor has been found;
      print($\gcd((b!P)_x - 1, N)$)
    end
  else
    $b = b + 1$;
  end
end

Algorithm 2: To factorize an integer N

Note that optimally we want the point $P \in C_m(\mathbb{Z}/N\mathbb{Z})$ to have high order in $C_m(\mathbb{Z}/N\mathbb{Z})$. However we cannot be sure of the order because the group structure of $C_m(\mathbb{Z}/N\mathbb{Z})$ relies on the prime factors of N.

Lemma 4.6. *Let $n, l \in \mathbb{Z}$ where n and l are pairwise coprime. Then:*

$$C_m(\mathbb{Z}/nl\mathbb{Z}) \simeq C_m(\mathbb{Z}/n\mathbb{Z}) \times C_m(\mathbb{Z}/l\mathbb{Z})$$

Proof. The map is given by:

$$\phi((a,b)) = ((a \bmod (n), b \bmod (n)), (a \bmod (l), b \bmod (l)))$$

Now we show that ϕ is indeed a homomorphism and bijective:
I.

$$\begin{aligned}\phi((1,0)) &= ((1 + k * nl, 0) \bmod n, (1 + k * nl, 0) \bmod l) \\ &= ((1,0) \bmod l, (1,0) \bmod l))\end{aligned}$$

II.

$$\begin{aligned}\phi((a_1,b_1) \oplus (a_2,b_2)) &= ((a_1a_2 + db_1b_2, a_1b_2 + a_2b_1) \bmod n, (a_1a_2 + db_1b_2, a_1b_2 + a_2b_1) \bmod l \\ &= ((a_1,b_1) \bmod n, (a_1,b_1) \bmod l) \oplus ((a_2,b_2) \bmod n, (a_2,b_2) \bmod l) \\ &= \phi((a_1,b_1)) \oplus \phi((a_2,b_2))\end{aligned}$$

So ϕ is indeed a homomorphism. Surjectivity is shown as follows: Let $((a_1,b_1),(a_2,b_2)) \in C_m(\mathbb{Z}/n\mathbb{Z}) \times C_m(\mathbb{Z}/l\mathbb{Z})$. Note, by Bezout's theorem since n, l are coprime, there exist integers t and s such that nt+ls=1.

Then take $P = (a_1ls + a_2nt, b_1ls + b_2nt) \in C_m(\mathbb{Z}/nl\mathbb{Z})$. Now to show that P is in the group:

$$\begin{aligned}(a_1ls + a_2nt)^2 - m(b_1ls + b_2nt)^2 &= a_1^2l^2s^2 + 2a_1a_2lnst + a_2^2n^2t_2 - mb_1^2l^2s^2 \\ &\quad - 2mb_1b_2lnst - mb_2^2n^2t^2 \\ &= a_1^2l^2s^2 - mb_1^2l^2s^2 + a_2^2n^2t_2 - mb_2^2n^2t^2 \bmod ln \\ &= l^2s^2 + n^2t^2 \bmod ln \\ &= (ls + nt)^2 \bmod ln \\ &= 1 \bmod ln\end{aligned}$$

Hence $P \in C_m(\mathbb{Z}/nl\mathbb{Z})$. We also have that $\phi(P) = ((a_1,b_1),(a_2,b_2))$. So ϕ is surjective. Injectivity is done as follows: Suppose we have $(a_1,b_1),(a_2,b_2) \in C_m(\mathbb{Z}/nl\mathbb{Z})$ such that $\phi((a_1,b_1)) = \phi((a_2,b_2))$. This means:

$$(((a_1,b_1) \bmod n, (a_1,b_1) \bmod l) = ((a_2,b_2) \bmod n, (a_2,b_2) \bmod l$$

Then,

$$\begin{aligned}a_1 &\equiv a_2 \bmod n \text{ which implies } a_1 = a_2 + k_1n, k_1 \in \mathbb{Z} \\ a_1 &\equiv a_2 \bmod l \text{ which implies } a_1 = a_2 + k_2l, k_2 \in \mathbb{Z} \\ \text{Hence, } a_1 &\equiv a_2 \bmod nl \\ \text{Similarly, } b_1 &\equiv b_2 \bmod nl\end{aligned}$$

So we have that $(a_1,b_1) = (a_2,b_2)$ and hence ϕ is isomorphic, proving the statement. □

Theorem 4.7. *Let $n_1, ..., n_r \in \mathbb{Z}$ where $n_1, ..., n_r$ are pairwise coprime. Then:*

$$C_m(\mathbb{Z}/n_1...n_r\mathbb{Z}) \simeq C_m(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times C_m(\mathbb{Z}/n_r\mathbb{Z})$$

Proof. The proof requires induction where lemma 3.5 serves as the base case. As induction hypothesis, suppose that:

$$C_m(\mathbb{Z}/n_1...n_r\mathbb{Z}) \simeq C_m(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times C_m(\mathbb{Z}/n_r\mathbb{Z})$$

for $n_1, ..., n_r$ pairwise coprime. Then let n_{r+1} be pairwise coprime to $n_1, ..., n_{r-1}$ and n_r. But then n_{r+1} is coprime to $n_1 n_2 ... n_{r-1} n_r$. By lemma 3.5 we have:

$$C_m(\mathbb{Z}/n_1...n_r n_{r+1}\mathbb{Z}) \simeq C_m(\mathbb{Z}/n_1...n_r\mathbb{Z}) \times C_m(\mathbb{Z}/n_{r+1}\mathbb{Z})$$

Hence by assumption:

$$C_m(\mathbb{Z}/n_1...n_r n_{r+1}\mathbb{Z}) \simeq C_m(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times C_m(\mathbb{Z}/n_{r+1}\mathbb{Z})$$

□

Hence the order of points in $C_m(\mathbb{Z}/N\mathbb{Z})$ will depend on the prime divisors of N.

5 Rediscovering Williams' $p+1$ method

Williams' $p+1$ method also tends to find factors of integers where either $p-1$ or $p+1$ is smooth. In fact a really interesting relation exists between this method and the factorisation algorithm based on Pell Conics. The Lucas functions discussed in section 2.2 actually represent points on a Pell conic:

Theorem 5.1. *Let U_n, V_n be the Lucas functions for some quadratic polynomial $X^2 - Rx + 1$, $R \in \mathbb{Z}$, where $U_n = U_n(R), V_n = V_n(R)$ and let $\Delta = R^2 - 4$. Then:*

$$\left(\frac{V_n}{2} \bmod N, \frac{U_n}{2} \bmod N\right) \in C_\Delta(\mathbb{Z}/N\mathbb{Z})$$

Proof. Taking $(X, Y) = \left(\frac{V_n}{2}, \frac{U_n}{2}\right) \bmod N$, plugging this into the Pell conic C_Δ we find:

$$X^2 - \Delta Y^2 = \frac{1}{4}(\alpha^n + \beta^n)^2 - \frac{1}{4}\Delta\frac{(\alpha^n - \beta^n)^2}{\Delta} = \frac{1}{4}4\alpha^n\beta^n = 1 \ (\alpha\beta = 1),$$
$$\text{where } x^2 - Rx + 1 = (x - \alpha)(x - \beta)$$

□

Hence for any $n \in \mathbb{N}$, the Lucas functions provide a point on the Pell conic, $\left(\frac{V_n}{2} \bmod N, \frac{U_n}{2} \bmod N\right) \in C_\Delta(\mathbb{Z}/N\mathbb{Z})$. Not only that but we can also prove the following:

Theorem 5.2. *Take* $\frac{V_n}{2}, \frac{U_n}{2}, \frac{V_m}{2}, \frac{U_m}{2} \in \mathbb{Z}/N\mathbb{Z}$ *such that* $\left(\frac{V_n}{2}, \frac{U_n}{2}\right), \left(\frac{V_m}{2}, \frac{U_m}{2}\right) \in C_\Delta(\mathbb{Z}/N\mathbb{Z})$ *for some* $n, m \in \mathbb{N}$. *Then:*

$$\left(\frac{V_n}{2}, \frac{U_n}{2}\right) + \left(\frac{V_m}{2}, \frac{U_m}{2}\right) = \left(\frac{V_{n+m}}{2}, \frac{U_{n+m}}{2}\right)$$

Proof.

$$\begin{aligned}
\left(\frac{V_n}{2}, \frac{U_n}{2}\right) + \left(\frac{V_m}{2}, \frac{U_m}{2}\right) &= \left(\frac{1}{4}(\alpha^{n+m} + \beta^m\alpha^n + \alpha^m\beta^n + \beta^{n+m}) + \frac{1}{4}(\alpha^n - \beta^n)(\alpha^m - \beta^m), *\right) \\
&= \left(\frac{1}{4}(2\alpha^{n+m} + 2\beta^{n+m}), *\right) \\
&= \left(\frac{V_{n+m}}{2}, *\right) \\
\text{Where } * &= \frac{1}{4}\left(\frac{\alpha^{n+m} - \alpha^n\beta^m + \alpha^m\beta^n - \beta^{n+m}}{\alpha - \beta}\right) \\
&\quad + \frac{1}{4}\left(\frac{\alpha^{n+m} + \alpha^n\beta^m - \alpha^m\beta^n - \beta^{n+m}}{\alpha - \beta}\right) \\
&= \frac{1}{4}\frac{2\alpha^{n+m} - 2\beta^{n+m}}{\alpha - \beta} \\
&= \frac{U_{n+m}}{2}
\end{aligned}$$

□

Now an alternative proof for Lehmer's theorem can be given:

Proof of theorem 4.1. Let p be an odd prime and $\left(\frac{\Delta}{p}\right) = \epsilon$, where $\Delta = (R^2 - 4)$. Previously we showed that $\left(\frac{V_n}{2}, \frac{U_n}{2}\right) \in C_\Delta(\mathbb{Z}/p\mathbb{Z})$, for $n \in \mathbb{N}$. Specifically if $m \in \mathbb{Z}_{>0}$, then $\left(\frac{V_{(p-\epsilon)m}}{2}, \frac{U_{(p-\epsilon)m}}{2}\right) \in C_\Delta(\mathbb{Z}/p\mathbb{Z})$. The order of $C_\Delta(\mathbb{Z}/p\mathbb{Z})$ will be $p-1$ if Δ is a quadratic residue mod p, and will be $p+1$ if Δ is not a quadratic residue mod p. Therefore $(p - \epsilon)m$ is a multiple of the order of $C_\Delta(\mathbb{Z}/p\mathbb{Z})$. By Lemma 3.3 we find:

$$\left(\frac{V_{(p-\epsilon)m}}{2}, \frac{U_{(p-\epsilon)m}}{2}\right) = (p - \epsilon)m\left(\frac{V_1}{2}, \frac{U_1}{2}\right) \equiv (1, 0) \bmod p$$

This means:

$$\begin{aligned}
\frac{V_{(p-\epsilon)m}}{2} &\equiv 1 \bmod p \\
\frac{U_{(p-\epsilon)m}}{2} &\equiv 0 \bmod p
\end{aligned}$$

Hence,

$$\begin{aligned}
V_{(p-\epsilon)m} &\equiv 2 \bmod p \\
U_{(p-\epsilon)m} &\equiv 0 \bmod p
\end{aligned}$$

□

In fact, our factorisation algorithm is a geometric interpretation of Williams' $p+1$ method. A rediscovery of the $p+1$ method has been found that does not require the Lucas Functions and instead functions by applying basic group theory rules. Now that the structure of this algorithm is evident, attempts can be made to make this algorithm more competitive with other methods.

6 Speeding up the factorisation algorithm based on Pell conics

Seeing that this algorithm is in fact a rediscovery of the $p+1$ method, speeding up the factorisation algorithm based on Pell conics will therefore be very similar, if not the same, as speeding up Williams' p+1 method. A few of these methods are discussed below.

6.1 Fast scalar multiplication

Previously it was noted that for the factorisation algorithm, only the x-coordinate is needed. The y-coordinate can therefore by discarded, and in fact, to find the x-coordinate of the sum of two points, only the x-coordinate is needed as well. To see this, consider $P = (x_P, y_P), Q = (x_Q, y_Q) \in C^m(\mathbb{Z}/p\mathbb{Z})$. Then:

$$P + Q = (x_P, y_P) + (x_Q, y_Q) = (x_P x_Q + m y_P y_Q, x_P y_Q + x_Q y_P)$$

But we also have:

$$P - Q = (x_P, y_P) + (x_Q, -y_Q) = (x_P x_Q - m y_P y_Q, x_P y_Q + x_Q y_P)$$

Hence, to find the x-coordinate of $P + Q$, we only need x_{P-Q}, x_P, x_Q:

$$x_{Q+P} = 2x_P x_Q - x_{Q-P}$$

Let (x_n) define the sequence of $x-$coordinates of multiples of P, i.e. $(x_0, x_1, x_2, ...) = (1, P_x, (2P)_x, ...)$. Let $Q = nP$ and $P = mP$, where $n, m \in \mathbb{Z}$. Then we find the recurrence relation:

$$\begin{aligned} x_{(n+m)P} &= 2x_{nP}x_{mP} - x_{(n-m)P} \\ x_{n+m} &= 2x_n x_m - x_{n-m} \end{aligned} \tag{2}$$

The P is removed since at this point we only consider multiples of P. So we have confirmed that the y-coordinate can be safely discarded as it is not required to compute multiples of $P \in C^m(\mathbb{Z}/p\mathbb{Z})$. Also note that the recurrence relation is not dependent on m for the conic $C^m(\mathbb{Z}/p\mathbb{Z})$. Alternatively to finding a random point $P \in C^m(\mathbb{Z}/p\mathbb{Z})$ for random m, described in the sketch in section 4.2.2, one can take a random integer $x \in [2, N-2]$. There is always a $y \in \mathbb{Z}/N\mathbb{Z}$, such that $(x, y) \in C_m(\mathbb{Z}/N\mathbb{Z})$ for at least one m. To prove this let $x \in [2, N-2]$. Then:

$$y^2 = \frac{x^2 - 1}{m}$$

If x^2-1 is coprime to N, then let m be $m = \frac{1}{(x^2-1)}$. Then $(x,1) \in C_m(\mathbb{Z}/N\mathbb{Z})$. If x^2-1 is not coprime to N then $\gcd(x^2-1, N) = a$ for some $a \neq 1$. Then we just found a non-trivial divisor of N. This case is quite unlikely but good to note.

The above recurrence relation (2) can now be used to create fast addition chains.

6.2 The Binary Method

Montgomery introduces in [8] a faster addition method when we have a recurrence relation of the form:

$$x_{n+m} = f(x_n, x_m, x_{n-m})$$

Where f is a continuous function. But equation (2) is exactly such a function. Note that any x_{n+m} can be computed as long as x_n, x_m and x_{n-m} are known. In the Binary Method we permit the difference between n and m to be either 0 or 1. Initially the x-coordinates x_1, x_2, x_3 are computed and stored for $P, 2P$ and $3P$ respectively. Then multiples x_n can recursively be computed with x_m and x_{m+1} where $m = \lfloor n/2 \rfloor$. Then x_m can be computed the same way, iterated until we reach x_1, x_2 or x_3. Let $L^b(n)$ denote the number of uses of (2) required to compute x_n. Montgomery finds in [8] that:

$$L^b(n) = \begin{cases} 2\log(n) - 1 & \text{if } n < 3 \cdot 2^{\log(n)-1} \\ 2\log(n) & \text{if } n \geq 3 \cdot 2^{\log(n)-1} \end{cases}$$

Computing the x-coordinate of nP using the group law requires n iterations. Hence, less iterations are required to compute the x-coordinate of nP. The code can be found in the appendix. This allows the computer to easily compute the x-coordinate of large multiples such as $500!P$. However, this is still not the fastest addition chain. Computing x_{m+n} we only permit a difference of either 1 or 0 between m and n. To illustrate the potential of our recurrence relation suppose that we want to compute x_{13}. The Binary method would compute x_{13} by the addition chain $x_1, x_2, x_3, x_4, x_6, x_7, x_{13}$, needing 7 iteration. However the optimal addition chain is in fact $x_1, x_2, x_3, x_5, x_8, x_{13}$ needing only *six* iterations. Here we permit the difference between m and n to be 3 or more. Faster addition chains exist using continued fractions (see [8, section 5]).

6.3 Stage 2 to conic factoring

A stage 2 is often applied to methods such as Pollard's $p-1$ method, and Williams' $p+1$ method (see [7, sections 4,5 and 6]). Say we have computed a large multiple of P, nP. In Stage 2, it is assumed that n is a multiple of $p-1$ except for one large prime factor, call it s. Then $p \pm 1 = Qs$ ($\pm$ based on the group order of $C_m(\mathbb{Z}/p\mathbb{Z})$) for some $Q \in \mathbb{Z}_{>0}$ where $Q \mid n$. If this is the case, computing the multiple gives:

$$s(nP) = \frac{n}{Q}(QsP) \equiv (1,0) \bmod p$$

Hence $p \mid (x_{sn} - 1)$ and a non-trivial factor is most likely found with $\gcd(x_{sn} - 1, N)$. The challenge is to find s. Let us assume that all prime-factors of $p - 1$ except for s are smaller or equal to some bound B_0. Then another bound B_1 can be defined and in stage 2 all prime numbers $s \in [B_0, B_1]$ are tried. Computing snP one-by-one is very time consuming, but luckily this can be sped up significantly. The following lemma is necessary:

Lemma 6.1. *Let p be a prime number and $x, y \in \mathbb{Z}$. Then:*

$$p \mid \gcd(xy \bmod N, N) \Leftrightarrow p \mid \gcd(x \bmod N, N) \text{ and/or } p \mid \gcd(y \bmod N, N)$$

The proof is trivial so is left as an exercise to the reader. The following lemma is also necessary:

Lemma 6.2. *Let (x_m) be the sequence of $x-$coordinates for multiples of a point $P \in C_m(\mathbb{Z}/N\mathbb{Z})$ and let $x_n, x_k \in (x_m)$. Then:*

$$x_{n-k} = \frac{x_n}{x_k}$$

Proof. To prove this we can use the recurrence relation (2) from section 6.1 to compute:

$$x_n = x_{n-k+k} = 2x_{n-k}x_k - x_{-n}$$

Then using the fact that $x_{-n} = x_n$, and that m is not a square we get:

$$2x_{n-k}x_k = 2x_n \text{ and hence } x_{n-k} = \frac{x_n}{x_k}$$

□

To efficiently compute x_{sn}, start by re-writing $s = vw - u$, where $v, w, u \in \mathbb{Z}$. Let $nP = B$, and denote the x value of mB as b_m. Select w to be close to $\sqrt{B_1}$, $w \approx \sqrt{B_1}$. Let $v_0 = \lceil \frac{B_0}{w} \rceil$ and $v_1 = \lceil \frac{B_1}{w} \rceil$. Then store the values $b_u \bmod N$ where $0 \leq u < w$ and the values $b_{vw} \bmod N$ where $v_0 \leq v \leq v_1$. Then for each prime $s \in [B_0, B_1]$ we can compute the gcd by:

$$b_s - 1 = b_{vw-u} - 1 = \frac{b_{vw}}{b_u} - 1$$

Computing the $\gcd(b_{vw} - b_u, N)$ will then give the same non-trivial factor as $\gcd(b_s - 1, N)$ by theorem 6.1, since

$$(\frac{b_{vw}}{b_u} - 1) * b_u = b_{vw} - b_u$$

This will massively reduce the memory and computations needed to compute all values $s \in [B_0, B_1]$, since a table can be saved of values b_u and b_{vw} representing the primes instead of computing primes separately. Why w is chosen close to

$\sqrt{B_1}$ is explained by Montgomery in [7].

To reduce computations even more, u and vw can be chosen such that pairs of primes s_1, s_2 can be found where $s_{1/2} = vw \pm u$. Both gcd computations can then be combined into:

$$\gcd(b_{vw}^2 - b_u^2, N)$$

An algorithm has been constructed in *Sage*, incorporating everything discussed in this thesis.

7 Examples

Big composite numbers of the form $N = pq$ p, q prime are here attempted to be found by the computer program based on Pell conics. In section 4.2, it was confirmed that the y-coordinate can be safely discarded. Now, alternatively to the algorithm discussed in section 4.2.2 we take a random $x \in [2, N-1]$. As earlier noted the algorithm makes most sense for values m such that m is not a quadratic residue mod p.

Remark. *If m is quadratic residue modulo p, the method based on Pell conics reduces to a slower version of Pollard's $p-1$ method*

If a random integer x is taken, then the chance that this x coordinate with designated y value lies on a Pell conic $P \in C_m(\mathbb{Z}/N\mathbb{Z})$ where m is not a quadratic residue mod p is exactly $\frac{1}{2}$. This is because half of integers $m \in \mathbb{Z}/N\mathbb{Z}$ are a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$ and half are not. Therefore multiple values for x may have to be chosen to find a non-trivial factor. In practice we take a random x at most 4 times, then the chance is $\frac{15}{16}$ that at least one of those $x \in \mathbb{Z}/N\mathbb{Z}$ lies on a Pell conic C_m where m is a quadratic residue mod p. The following factors are obtained by running the program, found in the appendix, for different integers N. The factor p is found by the algorithm:

Integer N	Factor p	Other factor q	Run-time(s)
1333333333333333333	4363363	305574698537191	101.45
4559454071533639	1357278899	3359261	105
1970048572989576571	2357278249	835730179	103
1270043339081464043	1357277791	935728373	109

It is interesting to see that it is actually very rare for $p+1$ or $p-1$ to only contain small prime factors and instead quite common that there is only one big prime factor in $p \pm 1$. In around 4 out of 5 cases that I ran big composite numbers of the form pq which yielded non-trivial divisors, a non-trivial factor was found at stage 2. Of course the method still pales in comparison with the built in factorisation method from Sage. The examples given above were calculated almost instantly with Sage's built in factorisation method. There

are however integers that this algorithm can factor faster than Sage. Van der Sluis, a peer who has done work on primality testing, shows that $2^{3217} - 1$ and $2^{4423} - 1$ are both prime numbers in [13, section 4], where $2^{4423} - 1$ has roughly 1331 digits. The algorithm on Pell conics was able to easily factorise the product $(2^{3217} - 1)(2^{4423} - 1)$ in 3 minutes whereas Sage's algorithm was not able to complete as it ran out of memory.

8 Discussion

Algorithms such as Pollard's $p-1$ method, and Williams' $p+1$ combined with trial testing are usually attempted first when factoring integers as they are quite fast at finding factors for very special prime factors, namely prime factors such that $p \pm 1$ is smooth. For example, prime factors of the form $M_n = 2^n - 1$, also known as the Mersenne Numbers can be found quickly using our factorisation algorithm. Afterwards more sophisticated methods are attempted. Unfortunately this program based on Pell conics is no different, making applications of this algorithm quite limited. The major flaw this method has is that for any integer m, $C_m(\mathbb{Z}/N\mathbb{Z})$ either has order $p-1$ or $p+1$. This means that if $p \pm 1$ is not (semi-)smooth, this algorithm would not be much faster compared to trial division. Lenstra's elliptic curve algorithm [3], that is based on elliptic curves, is in this aspect superior as the order of your group changes when a different elliptic curve is chosen. Elliptic curves are more complicated curves compared to Pell conics so it would be interesting to investigate algorithms based on third degree polynomials such as Lenstra's elliptic curve method.

Improvements in the addition chain the thesis uses, can also be made. It was explained in section 6.2 that the Binary method is not the fastest as it only allows a difference of either 1 or 0 between computing multiples of nP. In the end the computer program spent the most time on computing stage 2 of the algorithm. Perhaps adjustments in the code can be made to make this section of the code faster as well.

Integer factorisation is not the only application the group law over Pell conics has. Pell conics can also be used to prove that certain integers are prime. Peers from previous years (see [2, 13]) show how Pell conics can be used for primality testing. They test integers of the form $2^n - 1, 3 \cdot 2^n + 1, 3 \cdot 2^n - 1, n \in \mathbb{Z}_{>0}$ and provide conditions for when they are prime using Pell conics.

9 Appendix

Listing 1: Computer program in Sage computing a factor of an integer N

```
%time
sys.setrecursionlimit(6000)
def frec(xm,xn,xm_n,N):  #To compute x_(m+n)
    return ((2*xm*xn)%N-xm_n%N)%N

def iseven(n):
    if n%2==0:
        return True
    else:
        return False

def binaryt(n,N):  #For computing nP in some conic mod N
    global my_ev
    if n in my_ev:
        return my_ev[n]
    else:
        m=n//2
        if iseven(n):
            xm=binaryt(m,N)
            my_ev[n]=frec(xm,xm,1,N)
            return my_ev[n]
        else:
            my_ev[n]=frec(binaryt(m,N),binaryt(m+1,N),my_ev[1],N)
            return my_ev[n]

def get_primes(B0,B1):   #Stage 2 factorization
    prime_list=[]
    P=Primes()
    for i in range(B0,B1+1):
        if i in P:
            prime_list.append(i)
    return prime_list

def pair_primes(prime_list,w): #Algorithm that pairs primes in a range of primes
    prime_lists=prime_list[:]
    list_u=[]
    list_v=[]
    not_paired=[]
    while prime_lists != []:
        s=prime_lists[0]
        for i in prime_lists[1:]:
            if (s+i)%(2*w)==0:
                v=(s+i)/(2*w)
                u=v*w-s
                list_u.append(u)
                list_v.append(v)
                prime_lists.remove(i)
                prime_lists.remove(s)
                break
        if s in prime_lists:
            not_paired.append(s)
            v=s//w
```

```
            list_v.append(v)
            list_u.append(s-v*w)
            prime_lists.remove(s)
    return list_u,list_v,not_paired

N=1270043339081464043 #N, the integer to be factored

list_of_factors=[]  #The list of factors we found in N
xP=sage.misc.prandom.randint(2, N-1)  #Random integer, representing the initial point P
n=factorial(300)
my_ev={0:1,1:xP,2:frec(xP,xP,1,N),3:frec(frec(xP,xP,1,N),xP,xP,N)}
#The dictionary containing all computed x-values of multiples of P
for s in range(3,100):
    n=n*s
    nPx=binaryt(n,N)
    v=gcd(nPx-1,N)
    if v>1:
        if v!=N:
            print(v,nPx,n)
            list_of_factors.append(v)
            N=N//v
            break
        else:
            print("multiple of N")
            break
list_of_factors.append(N)
print(list_of_factors)

#Performing Stage 2
BP=my_ev[n]
print(BP)
my_new_ev={0:1,1:BP,2:frec(BP,BP,1,N),3:frec(frec(BP,BP,1,N),BP,BP,N)}
my_ev=my_new_ev
print(my_ev)

prime_list=prime_range(400, 1000000) #Generates a list of all primes in a range [B0,B1]
w=int(100000**0.5)
list_u,list_v,not_paired=pair_primes(prime_list,w)

print(len(list_v))
for i in range(len(list_v)):
    vw=int(list_v[i]*w)
    u=int(list_u[i])
    vwBPx=binaryt(vw,N)
    uBPx=binaryt(u,N)
    Ts=(vwBPx*vwBPx-uBPx*uBPx)%N
    if Ts!=0:
        f=gcd(Ts,N)
        if f>1:
            print(f)
%time
```

References

[1] D. J. Bernstein and T. Lange. Montgomery curves and the montgomery ladder. *IACR Cryptology ePrint Archive*, 2017:293, 2017.

[2] J. Dwarshuis. Primality testing, BSC Thesis, University of Groningen, 2017.

[3] N. Koblitz. *A course in number theory and cryptography*, volume 114. Springer Science & Business Media, 1994.

[4] D. H. Lehmer. An extended theory of lucas' functions. *Annals of Mathematics*, pages 419–448, 1930.

[5] F. Lemmermeyer. Conics-a poor man's elliptic curves. *arXiv preprint math/0311306*, 2003.

[6] F. Lemmermeyer. *Pell conics: An Alternative Approach to Elementary Number Theory, https://www.mathi.uni-heidelberg.de/ flemmermeyer/pell.html*. 2012.

[7] P. L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987.

[8] P. L. Montgomery. Evaluating recurrences of form. $X_{m+n} = f(X_m, X_n, X_{m-n})$, 1992.

[9] J. M. Pollard. Theorems on factorization and primality testing. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 76, pages 521–528. Cambridge University Press, 1974.

[10] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[11] S. A. Shirali. Groups associated with conics. *The Mathematical Gazette*, 93(526):27–41, 2009.

[12] R. Taton. L'≪essay pour les coniques≫ de pascal. *Revue d'histoire des sciences et de leurs applications*, 8(1):1–18, 1955.

[13] P. van der Sluis. Primality testing, BSC Thesis, University of Groningen, 2016.

[14] H. C. Williams. A p+ 1 method of factoring. *Mathematics of computation*, 39(159):225–234, 1982.