



hpvond

# New Families of ECM Curves for Cunningham Number

Eric Brier – ANTS IX – July 2010

# Summary

---



- 1 Seminal Idea
- 2 Associated modular curves
- 3 Parametric representations
- 4 Search for non-zero rank curves
- 5 Practical factorization
- 6 Conclusion

# Introduction to ECM



- Among several integer factoring algorithms, the Elliptic Curve Method allows to find medium-size prime factors (up to 70 decimal digits) in sub-exponential time and its running time mainly depends on the size of the factor.
- The sketch of the method is to compute a scalar multiplication of a point on the curve modulo  $n$ , as if  $n$  was a prime. Since it is not the case, something bad could happen during divisions, but then a factor is found.
- The basic idea is to look for a curve modulo  $n$ , which order once reduce modulo the factor  $p$  is smooth.

# Introduction to ECM



- Since we try to produce elliptic curves with a smooth order, a natural optimization is to build curves that do have a non trivial torsion subgroup over the field of rationals. The reduction modulo  $p$  of the curve does not annihilate this torsion subgroup.
- By doing this, we try to build a smooth number that is slightly smaller than the factor we are looking for. In most classical implementations, the reduction factor is chosen to be 12 or 16.

# Seminal Idea



- These reduction factors 12 and 16 are the largest sizes of torsion subgroups for elliptic curves over the field of rationals, as stated by a theorem of Mazur.
- Our idea is to work over number fields (i.e. algebraic extensions of the rationals) to obtain larger reduction factors.
- More precisely, the number field we consider are cyclotomic fields (i.e. extensions with roots of unity). These cyclotomic fields inject quite easily into  $\mathbb{Z}/n\mathbb{Z}$  when  $n$  has the following form:  $a^n \pm b^n$ .



# Need for infinite families



- Since ECM principle is to play with a sub-exponential number of curves, one needs to ensure that an infinite number of curves is available of a prescribed torsion subgroup.
- The set of isomorphism classes of elliptic curves with an order  $m$  torsion point is in one-to-one correspondence with an algebraic curve, which is usually denoted  $X_1(m)$ .
- This can be generalized to classes of elliptic curves with non-cyclic torsion subgroups, resulting in the study of the algebraic curve  $X_1(m_1, m_2)$ .

# Genus of modular curves



- As soon as the genus of a curve defined over a number field is strictly greater than one, the number of points of this curve is finite, which is incompatible with our application.
- We will thus focus on modular curves whose genus is at most one (in fact, as we will see later, we make use only of genus zero modular curves).
- Genus of  $X_1(m)$  or  $X_1(m_1, m_2)$  is easy to compute for small values of  $m$ ,  $m_1$  and  $m_2$ . Moreover, genus of  $X_1(p)$  is at most one only when  $p \leq 11$ , which is a good start for classification.



# Genus zero modular curves



- Genus zero  $X_1(m)$  and/or  $X_1(m_1, m_2)$  are associated to the following torsion subgroups:

|                            |  |  |
|----------------------------|--|--|
| $\mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$   |  |
| $\mathbb{Z}/3\mathbb{Z}$ , | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$   |  |
| $\mathbb{Z}/4\mathbb{Z}$ , | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ |
| $\mathbb{Z}/5\mathbb{Z}$ , | $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$   |  |
| $\mathbb{Z}/6\mathbb{Z}$ , | $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
| $\mathbb{Z}/7\mathbb{Z}$   |  |  |
| $\mathbb{Z}/8\mathbb{Z}$ , | $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$   |  |
| $\mathbb{Z}/9\mathbb{Z}$   |  |  |
| $\mathbb{Z}/10\mathbb{Z}$  |  |  |
| $\mathbb{Z}/12\mathbb{Z}$  |  |  |

# Genus one modular curves



- Genus zero  $X_1(m)$  and/or  $X_1(m_1, m_2)$  are associated to the following torsion subgroups:

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

$$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

$$\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/11\mathbb{Z}$$

$$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/14\mathbb{Z}$$

$$\mathbb{Z}/15\mathbb{Z}$$

# Suitable torsion subgroups



- To have full  $\ell$ -torsion defined over the base field, this field must contain all roots of unity of order  $\ell$ . This is an easy consequence of the existence of the Weil pairing.
- This constraint suits particularly well with the integer we have in mind to factor. The Cunningham numbers have the property that roots of unity exist modulo their non-trivial factors.
- Modular curves of genus one (when of non zero rank) do not give enough freedom on the curve parameters to be able to select elliptic curves having themselves non-zero rank. They will thus not been studied further.

# Modular curves of interest



- We will now focus on the following modular curves:

|                            |  |  |
|----------------------------|--|--|
| $\mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$   |  |
| $\mathbb{Z}/3\mathbb{Z}$ , | $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$   |  |
| $\mathbb{Z}/4\mathbb{Z}$ , | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ |
| $\mathbb{Z}/5\mathbb{Z}$ , | $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$   |  |
| $\mathbb{Z}/6\mathbb{Z}$ , | $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ , | $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
| $\mathbb{Z}/7\mathbb{Z}$   |  |  |
| $\mathbb{Z}/8\mathbb{Z}$ , | $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$   |  |
| $\mathbb{Z}/9\mathbb{Z}$   |  |  |
| $\mathbb{Z}/10\mathbb{Z}$  |  |  |
| $\mathbb{Z}/12\mathbb{Z}$  |  |  |

# Summary

---



- 1 Seminal Idea
- 2 Associated modular curves
- 3 Parametric representations
- 4 Search for non-zero rank curves
- 5 Practical factorization
- 6 Conclusion

# Parametric representations.



- "Good models" of modular curves have been deeply studied and many publications on that topic are available. Most of them make use of modular forms.
- Not being very familiar with spaces of modular forms, we followed an algebraic and incremental approach (i.e. building step by step modular representations of higher index).
- The modular curves we are interested in suit particularly well this approach.

# The curve $X_1(3,3)$



- A most common name for this curve is simply  $X(3)$ .
- We have the following sequence of covers:

$$X(3) \longrightarrow X_1(3) \longrightarrow X_0(3) \longrightarrow X_0(1)$$

- The maximal degree in this chain is 4.
- By using successive change of variable (centered on singularities), we get the following model for curves with full rational 3-torsion:

$$\begin{cases} a = 48\lambda^4 (\tau^3 - 1) \\ b = 16\lambda^6 (\tau^6 - 20\tau^3 - 8) \end{cases}$$

# The curve $X_1(6,3)$



- This curve is a 3-cover of the previous curve  $X(3)$ .
- A few algebraic steps end in the following parametric representation for elliptic curves:

$$\begin{cases} a = -3\lambda^4 (\tau^{12} - 8\tau^9 + 240\tau^6 - 464\tau^3 + 16) \\ b = -2\lambda^6 (\tau^{18} - 12\tau^{15} - 480\tau^{12} + 3080\tau^9 - 12072\tau^6 + 4128\tau^3 + 64) \end{cases}$$

- One can note that the curves can be defined over the rationals, while the torsion points are defined over a quadratic cyclotomic field.





# The curve $X_1(5,5)$



- We followed here a different approach by first imposing two rational torsion subgroups of order 5.
- We built a polynomial whose roots are the sum of the  $x$  coordinates of points of the groups of 5-torsion:

$$\chi_5(z) = z^6 + 20az^4 + 160bz^3 - 80a^2z^2 - 128abz - 80b^2$$

- Fixing two roots of this polynomial, we get two equations in the variables  $a$  and  $b$ . The variable  $a$  can then be easily eliminated.

# The curve $X_1(5,5)$



- After some more algebraic steps, we get a parametric representation for the parameters  $a$ ,  $b$  and both roots  $z_1$  et  $z_2$ .
- When then study the 5-division polynomial. By construction it has two quadratic factors and we can apply classical techniques of conic parameterization to get this representation of curve with full rational 5-torsion:

$$\begin{cases} a = -27\lambda^4 (\tau^{20} + 228\tau^{15} + 494\tau^{10} - 228\tau^5 + 1) \\ b = -54\lambda^6 (\tau^{30} - 552\tau^{25} - 10005\tau^{20} - 10005\tau^{10} + 522\tau^5 + 1) \end{cases}$$

# Summary

---



- 1 Seminal Idea
- 2 Associated modular curves
- 3 Parametric representations
- 4 Search for non-zero rank curves
- 5 Practical factorization
- 6 Conclusion

# Search for non-zero rank curves



- Now that we have at hand elliptic curves with the desired torsion sub-groups, we have to extract a sub-family of curves having non zero-rank, since we need a point of infinite order to launch the Elliptic Curve Method.
- We used some *ad-hoc* method, based on iterated changes of variables to reach the target.
- The main concern of this method is that we have no information on existence of non-zero rank curves when the method fails.

# Family of suitable curves with 4x4 torsion



- The curve parameters are:

$$\begin{cases} a = -27 (\nu^{16} + 24\nu^{14} + 476\nu^{12} + 4200\nu^{10} + 18022\nu^8 \\ \quad + 37800\nu^6 + 38556\nu^4 + 17496\nu^2 + 6561) \\ b = -54 (\nu^{24} + 36\nu^{22} + 66\nu^{20} - 6732\nu^{18} - 101409\nu^{16} - 707256\nu^{14} - 2772260\nu^{12} \\ \quad - 6365304\nu^{10} - 8214129\nu^8 - 4907628\nu^6 + 433026\nu^4 + 2125764\nu^2 + 531441) \end{cases}$$

- The point of infinite order is given by:

$$\begin{cases} x = \frac{3}{4\nu^2} (3\nu^{12} + 34\nu^{10} + 117\nu^8 + 316\nu^6 + 1053\nu^4 + 2754\nu^2 + 2187) \\ y = \frac{27}{8\nu^3} (\nu^2 - 3)(\nu^2 + 1)(\nu^2 + 9)(\nu^6 + 5\nu^4 + 15\nu^2 + 27)^2 \end{cases}$$

## Other torsion sub-groups



- To get 18 torsion points, we find a family related to a genus one curve, whose rank is luckily non zero. The elliptic curves used by ECM for factorization are then in one-to-one correspondence with points on an auxiliary elliptic curve.
- Our method totally failed in exhibiting a family of curve with non-zero rank and  $5 \times 5$  torsion. In fact, we even did not produce a single curve.
- Last, we built a family of curves with non-zero rank,  $4 \times 4$  torsion and “better probability” of yielding  $8 \times 4$  torsion.

# Summary

---



- 1 Seminal Idea
- 2 Associated modular curves
- 3 Parametric representations
- 4 Search for non-zero rank curves
- 5 **Practical factorization**
- 6 Conclusion



# Practical Factorizations



- We developed our own implementation of ECM, based on the families of elliptic curves we identified and make it run on Cunningham numbers.
- The most remarkable factors we got are:

$$5546025484206613872527377154544456740766039233 | 2^{1048} + 1$$

$$1581214773543289355763694808184205062516817 | 2^{972} + 1$$

# Summary

---



- 1 Seminal Idea
- 2 Associated modular curves
- 3 Parametric representations
- 4 Search for non-zero rank curves
- 5 Practical factorization
- 6 Conclusion

# Conclusion



- One can first note that the limitation on modular curve genera to zero does not allow torsion sub-group orders larger than 25.
- The factorization results obtained with the families of curves are re-insuring about some hidden bad properties that would have made them unsuitable for ECM.
- As pointed out by referees, some individual curves would be useful for the sieving part of SNFS algorithm. This will be subject of further research.

# Related Open Problems



- Find a more formal method to identify sub-families with non-zero rank.
- Find a non-zero rank family with  $5 \times 5$  torsion, or at least a single curve.
- Establish results on the ECM speed-up of these curves (maybe working on Chebotaref-like theorem).
- Find a different approach to allow usage of genus one modular curves and obtain larger torsion sub-group (maybe by finding method of constructing a point on the curve modulo  $n$ , which could be easier than factoring).

# Thank you for your attention

---



Details are given in the proceedings.

Your questions are welcome.