ELLIPTIC CURVES OF NEARLY PRIME ORDER.

DANIELE DI TULLIO, MANOJ GYAWALI

Abstract. Constructing an elliptic curve of prime order has a significant role in elliptic curve cryptography. For security purposes, we need an elliptic curve of almost prime order. In this paper, we propose an efficient technique to generate an elliptic curve of nearly prime order. In practice, this algorithm produces an elliptic curve of order 2 times a prime number. Therefore, these elliptic curves are appropriate for practical uses. Presently, the most known working algorithms for generating elliptic curves of prime order are based on complex multiplication.
The advantages of the proposed technique are: it does not require a deep mathematical theory, it is easy to implement in any programming language and produces an elliptic curve with a remarkably simple expression.

1. Introduction

Elliptic curve cryptography (ECC) has become the cornerstone of the public key cryptosystems because of its relatively shorter keys and the ease of implementation. The security of ECC is based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), which is considered a hard problem if the elliptic curve is chosen carefully. To date, most effective attacks, in general, are the Shank's deterministic Baby Step Giant Step algorithm [8] and the relatively fast (but probabilistic) Pollard's Rho method. Efficient attacks exist for elliptic curves of special forms: the pairing based attacks like MOV based on Weil pairing [1], Frey-Rück [5] based on Tate pairing and Pohlig-Hellman attack [13].

Pohlig-Hellman reduces the problem of computing ECDLP (Or in general the DLP over an abelian group) to ECDLP over subgroups of prime order. If the group of points of an elliptic curve has a smooth order (i.e. product of small primes) then the problem reduces to computing ECDLP to those prime factors and hence can be recovered by using the Chinese Remainder Theorem. The estimated complexity is

$$O\left(\sum_{i=1}^{t} e_i(\log_2(n) + \sqrt{p_i})\right)$$

where $n = \prod_{i=1}^{t} p_i^{e_i}$ is the order of E.
This complexity is maximum when n is a prime number. The second best case is when $n = 2p$ where p is a prime number. The loss of complexity from the first case is just given by a factor $\frac{1}{\sqrt{2}}$.
The pairing-based attacks (like MOV) reduces the ECDLP to a discrete logarithm problem over finite fields. Therefore, ECDLP becomes equivalent to a DLP over a finite field which can be solved in a relatively efficient way by index calculus. Usually, this finite field is a large extension of the field of definition of the used elliptic curve and there is no advantage to solve DLP over this field. Only in particular cases

Key words and phrases. Elliptic Curve Cryptography(ECC), Elliptic Curve Discrete Logarithm Problem(ECDLP), Quadratic Twist, Trace of an Elliptic Curve.

(for example supersingular elliptic curves) the field extension is small and then these attacks are effective.
Another family of curves that are unsafe for cryptography is that of anomalous curves, where the cardinality of the set of the rational points is equal to the cardinality of the field of definition. There are efficient algorithms like [14] to solve the ECDLP in such elliptic curves.
In general, it is not difficult to produce elliptic curves which are neither supersingular or anomalous. On the other side, it is not immediate to produce elliptic curves with almost prime order. Therefore, an algorithm is needed to construct such type of curves. For cryptographic purposes, there are various CM method algorithms to construct an elliptic curve of prime order N, for example [2, 3]. These algorithms can generate such a curve in time $\tilde{O}((\log N)^4)$. The most efficient known algorithm has been developed by Broker and Stevenhagen in [10] whose complexity is $\tilde{O}((\log N)^3)$ under some heuristic assumptions. However, proving deterministically that the starting number N is prime requires a complexity $\tilde{O}((\log N)^4)$. All of these techniques work by first fixing the cardinality of the set of rational points to be a known prime number N and then constructing the correct prime p and a curve E defined over $\mathbb{F}_p$. In conclusion, they require deep tools from Number Theory which are difficult to implement. In contrast, we present an algorithm that is easy to implement and efficient in producing elliptic curves which are suitable for cryptographic purposes. Heuristically, the average complexity is $\tilde{O}((\log N)^4)$. This algorithm does not produce elliptic curves of prime order but yields elliptic curves whose order is $2p$ where p is prime.
In section 2, we commence from a theorem that calculates the number of rational points of a family of curves then we present an extension of it. Based on this theorem, we present an algorithm in section 3. In section 4, we compute the complexity under some heuristic assumptions.

2. Family of elliptic curves

In this section, we extend the theorem [8, Theorem 4.23], which is crucial to the algorithm 1 in section 3.

Theorem 2.1. [8, Theorem 4.23] *Let p be an odd prime and let $k \not\equiv 0 \mod p$. Let $t_p := p + 1 - \#E(\mathbb{F}_p)$, where E is the elliptic curve*

$$y^2 = x^3 - kx$$

and t_p is the trace of the elliptic curve E.

1. *If $p \equiv 3 \mod 4$, then $t_p = 0$.*
2. *If $p \equiv 1 \mod 4$, write $p = a^2 + b^2$, where a and b are integers with b even and $a + b \equiv 1 \mod 4$. Then*

$$t_p = \begin{cases} 2a \text{ if } k \text{ is a fourth power mod } p \\ -2a \text{ if } k \text{ is a square but not a fourth power mod } p \\ \pm 2b \text{ if } k \text{ is not a square mod } p. \end{cases}$$

The author has not determined the sign of the trace t_p when k is not a square mod p instead he has mentioned that this is much more delicate problem. We have calculated the sign for $p \equiv 5 \bmod 8$. The result is the following theorem.

Theorem 2.2. *Let p be an odd prime and let $k \not\equiv 0 \mod p$. Let $t_p := p+1-\#E(\mathbb{F}_p)$, where E is the elliptic curve*

$$y^2 = x^3 - kx$$

and t_p is the trace of the elliptic curve E.
Assume that k is not a square mod p. Suppose that $p \equiv 5 \mod 8$, write $b = 2b'$ where $b' \in \mathbb{N}$ and $b' \equiv 1 \mod 2$. Then

$$t_p = \begin{cases} -2b \text{ if } \frac{k}{2} \text{ is a 4th power} \mod p \text{ and } b' \equiv 1 \mod 4 \\ 2b \text{ if } \frac{k}{2} \text{ is a square but not a 4th power} \mod p \text{ and } b' \equiv 1 \mod 4 \\ 2b \text{ if } \frac{k}{2} \text{ is a 4th power} \mod p \text{ and } b' \equiv 3 \mod 4 \\ -2b \text{ if } \frac{k}{2} \text{ is a square but not a 4th power} \mod p \text{ and } b' \equiv 3 \mod 4. \end{cases}$$

In order to prove the Theorem 2.2, we require the following lemmas.

Lemma 2.3. [11, Algorithm 3.4] *Let $p \geq 5$ be a prime number such that $p = a^2 + b^2$, where b is even. Choose the sign of a so that*

$$a + b \equiv 1 \mod 4.$$

Let $k \in \mathbb{F}_p^*$ for which

$$k^{\frac{p-1}{4}} \equiv \frac{b}{a} \mod p$$

then the elliptic curve over $\mathbb{F}_p$ of equation

$$y^2 = x^3 - kx$$

has trace $t_p = 2b$.

Proposition 2.4. [4, Proposition 5.3] *Suppose $p = a^2 + b^2 \equiv 1 \mod 4$ is a prime number with b even. Then*

$$2^{\frac{p-1}{4}} \equiv \left(\frac{b}{a}\right)^{\frac{ab}{2}} \mod p.$$

Lemma 2.5. *Suppose that $p \equiv 5 \mod 8$ is a prime. Write*

$$p = a^2 + b^2$$

where a is odd and $b \equiv 2 \mod 4$. Then

$$2^{\frac{p-1}{4}} \equiv \frac{b}{a} \mod p \text{ if and only if } \frac{ab}{2} \equiv 1 \mod 4.$$

Proof. Suppose $p = a^2 + b^2 \equiv 5 \mod 8$ is a prime with a is odd and $b \equiv 2 \mod 4$. If $p \equiv 3, 5 \mod 8$ we have that $\left(\frac{2}{p}\right) = -1$, so $2^{\frac{p-1}{4}}$ is a 4th primitive root of unity. By Proposition 2.4, we have

$$\begin{aligned} 2^{\frac{p-1}{4}} &\equiv \left(\frac{b}{a}\right)^{\frac{ab}{2}} \mod p. \\ &\equiv \frac{b}{a} \mod p \iff \frac{ab}{2} \equiv 1 \mod 4. \end{aligned}$$

□

Lemma 2.6. *Let $p = a^2 + b^2 \equiv 5$ mod 8 be a prime number. Assume that $b \equiv 2$ mod 4. Let E be the elliptic curve*

$$y^2 = x^3 - 2x$$

defined over $\mathbb{F}_p$ and $t_p = p + 1 - \#E(\mathbb{F}_p)$ be the trace of E. Then

$$t_p = \begin{cases} -2b & \text{if } b \equiv 2 \mod 8 \\ 2b & \text{if } b \equiv 6 \mod 8. \end{cases}$$

Proof. If $b \equiv 6 \mod 8$ then $\dfrac{b}{2} \equiv 3 \mod 4$. Choose the sign of a for which $a + b \equiv 1$ mod 4, which implies $a \equiv 3 \mod 4$. It follows that

$$\frac{ab}{2} \equiv 1 \mod 4.$$

By Lemma 2.5 we have,

$$2^{\frac{p-1}{4}} \equiv \left(\frac{b}{a}\right) \mod p.$$

Now, by using the Lemma 2.3, the trace $t_p = 2b$. Similarly the lemma follows for the case when $b \equiv 2$ mod 8. □

Definition 2.7. [8] Let E an elliptic curve defined over a finite field $\mathbb{F}_p$ by the equation

$$y^2 = x^3 + Ax + B$$

Let $d \in \mathbb{F}_p^*$, then the elliptic curve E^d over $\mathbb{F}_p$ defined by

$$y^2 = x^3 + d^2Ax + d^3B$$

is called quadratic twist of E by d.

Proposition 2.8. [8, Exercise 4.10] *Let E an elliptic curve defined over a finite field $\mathbb{F}_p$. Let $d \in \mathbb{F}_p^*$. Then*

$$\mathrm{Trace}(E^d) = \begin{cases} \mathrm{Trace}(E) & \text{if } d \text{ is a square mod } p. \\ -\mathrm{Trace}(E) & \text{otherwise} \end{cases}$$

Now, we have all the ingredients to complete the proof of the Theorem 2.2.

Proof of the Theorem 2.2.
In particular, the theorem is true for $k = 2$ by the Lemma 2.6. For the general proof, suppose k is not a square mod p. Since 2 is also not a square mod p, we have $\frac{k}{2}$ is square mod p. Write $\frac{k}{2} \equiv r^2 \mod p$. Therefore, the elliptic curve

$$y^2 = x^3 - kx$$

is a quadratic twist by r of the curve

$$y^2 = x^3 - 2x.$$

$\frac{k}{2}$ is a fourth power if and only if r is square. Furthermore, if r is not a square mod p then $\frac{k}{2}$ is not a fourth power but a square mod p. Hence, by the proposition 2.8 and the Lemma 2.6, we have all the possible cases of the theorem. □

3. Algorithm

As we have discussed before, supersingular elliptic curves are vulnerable to pairing-based attacks. Therefore we will consider only the case in which $p \equiv 1 \mod 4$, more precisely the algorithm produces curves for which $p \equiv 5 \mod 8$. If we know the decomposition of the prime p as a sum of two squares then we also have the cardinality of $E(\mathbb{F}_p)$. Note that in our case this cardinality cannot be a prime number since the order of the elliptic curve is always an even number. The closest case to be a prime is when k is not a square $\mod p$, in which case $\#E(\mathbb{F}_p) \equiv 2 \mod 4$. Therefore, we can expect that $\#E(\mathbb{F}_p) = 2p'$, where p' is prime. If k is a square $\mod p$ then we can have $\#E(\mathbb{F}_p) = 4p'$, where p' is prime. These curves are resistant against Pohlig-Hellman attack.
Consider elliptic curves in Weierstrass form

$$y^2 = x^3 \pm 2x$$

and prime number $p \equiv 5 \mod 8$. In particular, we can take $p = 2^2 + m^2$. Theorem 2.2 ensures that the trace is always -4 for the case $k = 2$. Considering the quadratic twist by $\sqrt{-1} \mod p$, which is not a square when $p \equiv 5 \mod 8$, we deduce that the trace of

$$y^2 = x^3 + 2x$$

is always 4. Therefore, whenever we find a number of the form $2^2 + m^2$ is a prime p we can identify whether $\frac{p-3}{2}$ or $\frac{p+5}{2}$ is prime. If one of them is prime, then we obtain required elliptic curves i.e. in the former case the output is $y^2 = x^3 + 2x$ over $\mathbb{F}_p$ and in the later case the output is $y^2 = x^3 - 2x$ over $\mathbb{F}_p$.

Algorithm 1 Elliptic curve of almost prime order

```
m = m_0 {We choose m_0 ≡ 1 mod 2.}
B=true {A boolean variable.}
while B do
  p = 4 + m^2
  if Is Probable Prime(p) then
    pdash = (p − 3)/2
    if Is Probable Prime(pdash) then
      B=false
      Print("Elliptic Curve y^2 = x^3 + 2x over F_p)
    end if
    pbar=(p+5)/2
    if Is Probable Prime(pbar) then
      B=false
      Print("Elliptic Curve y^2 = x^3 − 2x over F_p)
    end if
  end if
end while
```

4. Complexity

The complexity of this algorithm is essentially based on the complexity of the primality test. The best known primality test is the Miller-Rabin primality test

based on Fast Fourier transform multiplication [12], which has estimated complexity

$$\tilde{\mathcal{O}}(c\log^2(n))$$

to determine whether n is prime or not. Here c is the maximum number of rounds of the test. Note that when n is not prime one expects that the number of rounds needed to end the algorithm is low.
We want to estimate the number of attempts needed to find a couple of prime numbers either $(p, \frac{p-3}{2})$ or $(p, \frac{p+5}{2})$. This is related to the following question:

"Given a number n, what is the probability that n is prime?"

Posing the question in this way is meaningless since we have to specify a finite set from which n is taken randomly. Instead, we pose the question in the following way:

"Given a number n of binary length l, what is the probability that n is prime?"

We recall a fundamental result from Analytic Number Theory:

Theorem 4.1 (Prime Number Theorem)**.** *Let*

$$\pi : \mathbb{N} \to \mathbb{N}$$

given by $\pi(n) := \#\{p \leq n : p \text{ is prime}\}$*. Then*

$$\pi(n) \sim \frac{n}{\ln(n)}.$$

This is just an asymptotic estimation, but it allows to expect that the set of prime numbers of length l, i.e.

$$\#\{2^{l-1} \leq p < 2^l - 1\} \sim \pi(2^l) - \pi(2^{l-1})$$

which implies

$$\pi(2^l) - \pi(2^{l-1}) \sim 2^{l-1} \cdot \frac{\log_2(e)}{l}.$$

Therefore, the probability that a number lying in this interval to be prime is around

$$\frac{\log_2(e)}{l}.$$

From this we can deduce the probability that given two numbers n_1, n_2 which are chosen randomly of length l none of them prime is approximately

$$\left(1 - \frac{\log_2(e)}{l}\right)^2$$

and the probability that at least one of them is prime is around

$$\frac{2\log_2(e)}{l}.$$

Therefore, the probability that at least one of the couples $(p, \frac{p+5}{2})$ and $(p, \frac{p-3}{2})$ is composed by prime numbers is around $\frac{2\log_2(e)^2}{l^2}$. If we repeat the iteration m times the probability of not getting a couple of prime numbers is around

$$\left(1 - \frac{2\log_2(e)^2}{l^2}\right)^m$$

Choosing $m \sim l^2$ we have that this probability is around $e^{-2\log_2(e)^2} \sim 0.015$, which is very low and thus we expect to find a couple in m attempts. It follows that the expected complexity to find a good elliptic curve is

$$\tilde{\mathcal{O}}(l^4)$$

under the heuristic of distributions of primes.

5. Acknowledgements

We greatly thank René Schoof and Carlo Pagano for their important suggestions to complete the mathematical part of this paper. We also thank Ankan Pal for reading our preprint and providing us useful suggestions.

References

[1] A. Menezes, T. Okamoto and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, *IEEE transactions on Information Theory*, 39(1993),1639-1646.

[2] E. Konstantinou, Y. C. Stamatiou, C. D. Zaroliagis, *On the construction of prime order elliptic curve, Progress in cryptology-INDOCRYPT* , *Springer Lecture Notes in Computer Science 2162*, (2001),142-158.

[3] E. Savas, T. A. Schmidt, C. K Koc, *Generating elliptic curve of prime order*, *Cryptographic hardware and embedded system-CHES 2001(Paris), Springer Lecture Notes in Computer Science 2162*, (2003),309-322.

[4] F. Lemmermeyer *Receprocity laws*, Springer Monographs in Mathematics, 2000.

[5] G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, *Mathematics of computation*, 62(1994),865-874.

[6] I. A. Semaev. *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p.* Math. Comp., 67(1998),353-356.

[7] J. Pollard, *Monte Carlo methods for index computation mod p*, *Mathematics of Computation*, 32(1978),918-924.

[8] Lawrence C. Washington, *Elliptic curves number theory and cryptography* , *Chapman and Hall/CRS*, (2008).

[9] Rabin, M. (1980). *Probabilistic algorithm for testing primality. Journal of Number Theory*, 12 (1980), 128-138.

[10] Reinier Broker,Peter Stevenhagen, *Efficient CM-construction of elliptic curves over finite field*, Mathematics of computation, 76 (2007).

[11] Rubin, Karl and Silverberg, Alice, *Choosing the correct elliptic curve in the CM method*, *Math. Comp.* , 79(2010),545-561.

[12] Shyam Narayanan and David Corwin, *Improving the Speed and Accuracy of the Miller-Rabin Primality Test* (2015).

[13] S. Pohlig and M. Hellman, *An improved algorithm for computing logarithm over GF(p)*, *IEEE Transactions on Information Theory*, 24(1978),106-110.

[14] Takakazu Satoh and Kiyomichi Araki. *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves.* Comment. Math. Univ. St. Paul, 47(1998),81-92.

Roma Tre University, Department of Mathematics and Physics
Email address: danieleditullio@hotmail.it, manoj.gyawali@ncit.edu.np