

# Elliptic Curves with a Given Number of Points

Reinier Bröker and Peter Stevenhagen

Mathematisch Instituut, Universiteit Leiden,  
Postbus 9512, 2300 RA Leiden, The Netherlands  
`{reinier,psh}@math.leidenuniv.nl`

**Abstract.** We present a non-archimedean method to construct, given an integer  $N \geq 1$ , a finite field  $\mathbf{F}_q$  and an elliptic curve  $E/\mathbf{F}_q$  such that  $E(\mathbf{F}_q)$  has order  $N$ .

## 1 Introduction

A classical theorem of Hasse from 1934 states that for an elliptic curve  $E$  defined over the finite field  $\mathbf{F}_q$  of  $q$  elements, the order of the group  $E(\mathbf{F}_q)$  of  $\mathbf{F}_q$ -rational points is an integer in the *Hasse interval*

$$\mathcal{H}_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

around  $q$ . If  $E$  is given in some standard way, say by a Weierstrass equation over  $\mathbf{F}_q$ , there are several algorithms that compute the order of  $E(\mathbf{F}_q)$ . The 1985 algorithm by Schoof [8,9] runs in time polynomial in  $\log q$ , and in small characteristic  $p$  there are even faster  $p$ -adic algorithms due to Satoh [7] and Kedlaya [5].

The situation is rather different in the case of the following problem, which can be seen as an ‘inverse problem’ to the point counting problem.

**Problem.** *Given an integer  $N \geq 1$ , find a finite field  $\mathbf{F}_q$  and an elliptic curve  $E/\mathbf{F}_q$  for which the number of  $\mathbf{F}_q$ -rational points equals  $N$ .*

As with other inverse problems, such as in Galois theory, this is mathematically a natural question to ask. In this particular case, an efficient solution to the problem would also be desirable in view of the need in current applications to construct elliptic curves having point groups satisfying various smoothness requirements with respect to their order. It is one of the reasons why we focus on the order  $N$ , and do not specify the finite field  $\mathbf{F}_q$  as being part of the input. In addition, we will use the freedom with respect to the choice of a base field  $\mathbf{F}_q$  to our advantage.

A necessary condition for our problem to be solvable for given  $N$  is clearly that  $N$  is contained in *some* Hasse interval  $\mathcal{H}_q$ , so we would like the union  $\bigcup_q \mathcal{H}_q$  over all prime powers  $q$  to contain *all* positive integers. It is easy to see that the contribution to the union coming from the ‘true’ prime powers  $q$  that are not primes is negligible: it is contained in a zero density subset of  $\mathbf{Z}_{\geq 1}$ . For this reason, we may and will restrict in the sequel to the case where the base field  $\mathbf{F}_q$

is the prime field coming from a prime number  $q$ . In this particular case, all integers in  $\mathcal{H}_q$  actually do occur as the group order of  $E(\mathbf{F}_q)$  for some elliptic curve  $E$ , so  $N \in \mathcal{H}_q$  is sufficient to guarantee the existence of a solution. (For arbitrary prime powers  $q$  there are often not enough supersingular curves to realize all orders congruent to 1 modulo the characteristic.)

For the equality  $\mathbf{Z}_{\geq 1} = \bigcup_{q \text{ prime}} \mathcal{H}_q$  we need to show that the primes are not too far apart, i.e., that the gap between consecutive primes  $q$  and  $q'$  is roughly bounded by  $4\sqrt{q}$  for large  $q$ . This is more than what is currently known to be true: even under assumption of the Riemann hypothesis the gap between consecutive primes can only be shown to be of order  $O(\sqrt{q}(\log q)^2)$ . However, from a practical, algorithmic point of view there are always *lots* of primes  $q$  for which a large integer  $N$  is contained in  $\mathcal{H}_q$ . Indeed, by the prime number theorem, we expect 1 out of every  $\log N$  integers around  $N$  to be prime, so for large  $N$  the set of primes  $q$  having  $N \in \mathcal{H}_q$  is on average of size  $4\sqrt{N}/\log N$ , and finding such  $q$  is never a problem in practice.

Once we have found a prime  $q > 3$  for which we have  $N \in \mathcal{H}_q$  (we now require  $N > 1$ ), there is the following *naïve algorithm* to find an elliptic curve having exactly  $N$  rational points over  $\mathbf{F}_q$ . Suppose that we are not in the easy cases where we have  $N = q + 1$  (then any supersingular curve over  $\mathbf{F}_q$  will do) or where one of the few curves with  $j$ -invariant 0 or 1728 has the right number of points. Then we try

$$E_a : y^2 = x^3 + ax - a \quad \text{with} \quad j(E_a) = 1728 \frac{4a}{4a + 27}$$

for random  $a \in \mathbf{F}_q^* \setminus \{-\frac{27}{4}\}$  as the Weierstrass equation of the desired curve until we find a curve having  $N$  points. More precisely, we write  $N = q + 1 - t$  and check whether for our  $a$  the point  $(1, 1) \in E_a(\mathbf{F}_q)$  is annihilated by  $N = q + 1 - t$  or  $q + 1 + t$ . If it is, we check whether the number of  $\mathbf{F}_q$ -rational points is indeed  $q + 1 \pm t$ . For order  $N = q + 1 - t$  we are done, for order  $q + 1 + t$  not  $E_a$  itself but its quadratic twist has  $N$  points. Even though the distribution of the group orders of elliptic curves over  $\mathbf{F}_q$  is not quite uniform, we expect to examine  $O(\sqrt{q}) = O(\sqrt{N})$  curves  $E_a$  before we hit a curve having exactly  $N$  points. As the amount of time spent per  $a$  is usually very small, and certainly polynomial in  $\log N$ , this yields a probabilistic algorithm with expected running time  $O(N^{\frac{1}{2} + o(1)})$ . It is quite practical for small values of  $N$ , but becomes unwieldy for  $N \gg 10^{15}$ .

In the next section we briefly describe a classical deterministic algorithm based on complex multiplication methods which, although not asymptotically faster than the naïve algorithm, can be improved in various ways. Our first improvement is a  $p$ -adic approach to complex multiplication based on the recent work of Couveignes and Henocq [3]. It is described in section 3, and illustrated by the explicit computation in section 4 of an ‘ANTS 6 curve’ having 2004061320040618 rational points. Our second improvement, in section 5, consists of using ‘small’ modular functions in this  $p$ -adic context to push the limits of what is feasible by  $p$ -adic methods. Although the resulting algorithm is still far from polynomial, its power is illustrated in section 6 by the computation of an elliptic curve having  $10^{30}$  rational points.