Illinois Journal of Mathematics
Volume 48, Number 3, Fall 2004, Pages 1041–1052
S 0019-2082

# MOV ATTACK IN VARIOUS SUBGROUPS ON ELLIPTIC CURVES

FLORIAN LUCA, DAVID JOSE MIRELES, AND IGOR E. SHPARLINSKI

Abstract. We estimate the probabilities that the Menezes-Okamoto-Vanstone reduction of the discrete logarithm problem on an elliptic curve $\mathbb{E}$ to the discrete logarithm problem in a certain finite field succeeds for various groups on points on $\mathbb{E}$. Our bounds imply that in all interesting cases these probabilities are exponentially small. This extends results of Balasubramanian and Koblitz who have treated the instance in which the order of the group of points on $\mathbb{E}$ is prime.

## 1. Introduction

Let $\mathbb{E}$ be an elliptic curve defined over a finite field $\mathbb{F}_p$ of $p$ elements, where $p$ is a prime. Let $\mathbb{E}(\mathbb{F}_p)$ denote the set of $\mathbb{F}_p$-rational points on $\mathbb{E}$ (including the point at infinity $\mathcal{O}$). We recall that $\mathbb{E}(\mathbb{F}_p)$ forms an abelian group (with $\mathcal{O}$ as the identity element). Its cardinality $N = \#\mathbb{E}(\mathbb{F}_p)$ belongs to the *Hasse-Weil* interval, $N \in \mathcal{I}_p$, where

$$\mathcal{I}_p = [p + 1 - 2p^{1/2},\, p + 1 + 2p^{1/2}].$$

It is well-known that the group $\mathbb{E}(\mathbb{F}_p)$ is of the form $\mathbb{Z}_L \times \mathbb{Z}_M$, where the integers $L$ and $M$ are uniquely determined with $M \mid L$. Typically, in cryptographic applications, the curve $\mathbb{E}$ is chosen in such a way that $\mathbb{E}(\mathbb{F}_p)$ is a small multiple of a prime number. Unfortunately, it is not clear how to choose such curves, or whether some specific constructions of such curves introduce additional weaknesses in the corresponding *discrete logarithm problem*. In any case, the security of the cryptosystem depends on the presumed difficulty of solving the discrete logarithm problem in a maximal cyclic subgroup of $\mathbb{E}(\mathbb{F}_p)$ of prime order, which we denote by $Q$. The best known general discrete logarithm algorithms in the group $\mathbb{E}(\mathbb{F}_p)$ run in time about $Q^{1/2}$ (as for any other abelian group of the same order $N$).

A different algorithm that has been developed for the elliptic curve discrete logarithm is the well-known *Menezes-Okamoto-Vanstone* algorithm, MOV

Received January 18, 2004; received in final form April 8, 2004.
2000 *Mathematics Subject Classification.* 11N25, 11T71, 14H52.

(see [6]). This algorithm constructs an embedding of a fixed cyclic subgroup of order $L$ of $\mathbb{E}(\mathbb{F}_p)$ into the multiplicative group $\mathbb{F}_{p^k}^*$ of a suitable extension of $\mathbb{F}_p$. Heuristically, using the number field sieve, discrete logarithms in $\mathbb{F}_{p^k}^*$ can be found in running time $\mathcal{L}_{p^k}\left(1/3, (64/9)^{1/3}\right)$ by the number field sieve algorithm (see [2], [8], [9]), where, as usual, $\mathcal{L}_m(\alpha, \beta)$ denotes any quantity of the form

$$\mathcal{L}_m(\alpha, \beta) = \exp\left((\beta + o(1))(\log m)^{\alpha}(\log\log m)^{1-\alpha}\right).$$

In particular, it follows that in order for the running time for MOV (combined with the number field sieve) to be subexponential one needs $k \le \log^2 p$. One can, however, assume further progress in the discrete logarithm problem over finite fields, which may force to consider larger values of $k$. Thus, in this paper, we consider a more general situation where all values of $k$ up to a certain sufficiently large bound $K$ are considered as admissible.

It is known that two necessary and sufficient conditions for MOV to be carried out in $\mathbb{F}_{p^k}$ are that $L \mid (p^k - 1)$, and that there are $L^2$ points of order dividing $L$ in $\mathbb{E}(\mathbb{F}_{p^k})$.

It is also known that the second condition above implies the first one. Balasubramanian and Koblitz (see [1]), have showed that, conversely, the second condition above is also implied by the first one once $\mathbb{E}(\mathbb{F}_p)$ is cyclic of order $N$, a prime which does not divide $p-1$.

In the same paper [1], Balasubramanian and Koblitz give also an upper bound on the probability that a random pair $(p, \mathbb{E})$ consisting of a prime number $p$ in the interval $[x/2, x]$ and an elliptic curve $\mathbb{E}$ over $\mathbb{F}_p$ and having a prime number of points (thus, $\#\mathbb{E}(\mathbb{F}_p) = N = L = Q$) satisfies the condition that $N \mid (p^k - 1)$ for some $k \le \log^2 p$. They show that for a sufficiently large $x$ the above probability is $O\left(x^{-1}\log^9 x \log\log^2 x\right)$. This means that for a random elliptic curve with a prime number of points, MOV succeeds only with negligible probability.

It is certainly customary in cryptography to use elliptic curves with a prime or almost prime number of points. Unfortunately, the only known approach to generate elliptic curves with a prime number of points consists in performing repeatedly the following steps:

- choose a random curve $\mathbb{E}(\mathbb{F}_p)$;
- recall a point counting algorithm (which is a rather time consuming procedure) to compute $N = \#\mathbb{E}(\mathbb{F}_p)$;
- test $N$ for primality.

The relaxation of the primality condition to almost primality does not lead to any substantial speed up. Moreover, it is not even known whether for every prime $p$ one can find an elliptic curve over $\mathbb{F}_p$ with the desired arithmetic structure of the number of points, although certainly this fact has never been doubted in practice. Thus, in order to make a rigorous analysis of the above algorithm, one also needs to choose the prime $p$ at random, which leads to an additional primality testing at each round.

It is certainly interesting and useful to analyze MOV in other cases which may occur in various applications of elliptic curves. Here we concentrate on the case when the curve $\mathbb{E}$ is chosen at random from the set of all elliptic curves over $\mathbb{F}_p$ without any verification of the arithmetic structure of $\#\mathbb{E}(\mathbb{F}_p)$.

For such a "random curve" $\mathbb{E}$, we estimate the probabilities that MOV succeeds for each of the following cases:

- in the group of all points $\mathbb{E}(\mathbb{F}_p)$;
- in the largest cyclic subgroup of $\mathbb{E}(\mathbb{F}_p)$;
- in the largest cyclic subgroup of $\mathbb{E}(\mathbb{F}_p)$ of prime order.

We show that in all these cases the probability of success of MOV is exponentially small. Moreover, our results hold for every prime $p$ and a randomly chosen curve $\mathbb{E}$ over $\mathbb{F}_p$, while for the result of [1], additional randomisation over $p$ is essential.

In particular, we also extend the above result of [1] to the case in which $\mathbb{E}(\mathbb{F}_p)$ is cyclic but its number of points $N$ is no longer required to be a prime, and even to the general case in which we impose no restriction on the group structure of $\mathbb{E}(\mathbb{F}_p)$ at all.

As in [1], one of our basic tools is a result of Lenstra from [5], which essentially claims that every integer $N \in \mathcal{I}_p$ represents the cardinality $\#\mathbb{E}(\mathbb{F}_p)$ for approximately the same number of elliptic curves $\mathbb{E}$ over $\mathbb{F}_p$. This provides a link between our problem and the number-theoretical problem of studying integers in small intervals dividing $p^k - 1$ for a small $k$, a problem which is of independent interest and the study of which forms the backbone of our results.

Throughout this paper, we use the symbols '$O$', '$\ll$', '$\gg$', '$\asymp$' and '$o$' with their usual meaning (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$ and that $A \asymp B$ means that both $A \gg B$ and $A \ll B$ hold).

We use $\omega(n)$ for the number of distinct prime factors of the positive integer $n$ and we use $P(n)$ for the largest prime divisor of $n$, where we put $\omega(1) = 0$ and $P(1) = 1$. We denote by $\mathrm{rad}(n)$ the radical of $n$, that is, the largest squarefree divisor of $n$.

For a positive real number $x$ and a positive integer $k$ we use $\log_k x$ for the recursively defined function given by $\log_k x = \max\{\log(\log_{k-1} x),\ 1\}$, where log is the natural logarithm function. When $k = 1$, we omit the subscript, and we thus understand that all logarithms which will appear are $\geq 1$.

**Acknowledgements.** F. L. and D. M. were supported in part by Project PAPIIT IN-104602 UNAM, and I. S. was supported in part by ARC grant DP0211459.

## 2. Preparations

It is known that there are $2p + O(1)$ classes of non-isomorphic curves over $\mathbb{F}_p$ (see Section 1.4 of [5]). Proposition 1.9 of [5] asserts that their cardinalities are distributed in an almost uniform way up to some logarithmic factors.

Lemma 2.1. *For any integer $N \in \mathcal{I}_p$ the number of isomorphism classes of elliptic curves $\mathbb{E}$ over $\mathbb{F}_p$ with $N = \#\mathbb{E}(\mathbb{F}_p)$ is $O\left(p^{1/2} \log p \log_2^2 p\right)$.*

In what follows, we often use the fact that the inequality $\omega(n) < \log n$ holds for all sufficiently large integers $n$, which follows from the trivial inequality $\omega(n)! \le n$ and the Stirling formula.

For real numbers $H \ge h \ge 1$ and an integer $K \ge 1$, we let $\mathcal{N}(p, K, H, h)$ be the set of positive integers $N$ in the interval $[H - h, H + h]$ and such that $N \mid (p^k - 1)$ holds with some positive integer $k \le K$.

For an integer $w \ge 1$, we let $\mathcal{N}_1(p, K, H, h, w)$ and $\mathcal{N}_2(p, K, H, h, w)$ be the subsets consisting of $N \in \mathcal{N}(p, K, H, h)$ with $\omega(N) \le w$ and with $\omega(N) > w$, respectively. The next two results give upper bounds on $\#\mathcal{N}_1(p, K, H, h, w)$ and $\#\mathcal{N}_2(p, K, H, h, w)$, which we later use to estimate

$$\#\mathcal{N}(p, K, H, h) = \#\mathcal{N}_1(p, K, H, h, w) + \#\mathcal{N}_2(p, K, H, h, w)$$

for an optimally chosen value of $w$.

Lemma 2.2. *There exists a constant $C_1 > 0$ such that for any integer $w$ with $w \to \infty$ in such a way that $w \le 0.5K \log p$ the inequality*

$$\#\mathcal{N}_1(p, K, H, h, w) \ll K \left( \frac{C_1 K \log H \log p}{w} \right)^w$$

*holds.*

*Proof.* Let

$$N = \prod_{q \mid (p^k - 1)} q^{a_q}$$

be the prime number factorization of $N \in \mathcal{N}_1(p, K, H, h, w)$ with $N \mid (p^k - 1)$ for some $k \le K$. Then $N$ is supported on at most $w$ primes $q \mid (p^k - 1)$ and for these primes we have $2^{a_q} \le q^{a_q} \le N \le 2H$. Therefore $a_q \le 2 \log H / \log 2 < 3 \log H$, and we see that

$$\begin{aligned}\#\mathcal{N}_1(p, K, H, h, w) &\le \sum_{k=1}^{K} \sum_{s=0}^{w} \binom{\omega(p^k - 1)}{s} (3 \log H)^s \\ &\le (3 \log H)^w \sum_{k=1}^{K} \sum_{s=0}^{w} \binom{\omega(p^k - 1)}{s}.\end{aligned}$$

Clearly, the inequality $\omega(p^k-1) \le k \log p$ holds for all sufficiently large values of $p$. Therefore, we derive

$$\begin{aligned} \#\mathcal{N}_1(p,K,H,h,w) &\le Kw \binom{\lfloor K\log p\rfloor}{w} (3\log H)^w \\ &\le \frac{K}{(w-1)!}(3K\log H \log p)^w \end{aligned}$$

and the Stirling formula applied to $(w-1)!$ completes the proof. □

Lemma 2.3. *There exists a constant $C_2 > 0$ such that for any $w$ with $w \to \infty$ and $H \ge h$ the inequality*

$$\#\mathcal{N}_2(p,K,H,h,w) \le h\left(\frac{C_2 \log_2(K^2\log p)}{w}\right)^{w/2} + K\left(\frac{C_2 K \log p}{w}\right)^{w/2}$$

*holds for large values of the prime $p$.*

*Proof.* For each $N \in \mathcal{N}_2(p,K,H,h,w)$ we write $N = m\ell$, where $m$ is the product of the $v = \lfloor w/2 \rfloor$ smallest distinct prime factors of $N$. Note that $\ell \ge m$ because $N$ has at least $w$ distinct prime factors. We also have $H/m - h/m \le \ell \le H/m + h/m$. Therefore, for each fixed $m$, there are at most $O(h/m)+1$ values of $\ell$.

Let $\mathcal{Q}_k$ be the set of all prime factors of $p^k-1$, and let $\mathcal{M}_k$ be the set of all the squarefree integers $m$ having all their prime factors in $\mathcal{Q}_k$ and satisfying $\omega(m) = v$. We also put

$$\mathcal{M} = \bigcup_{k=1}^{K} \mathcal{M}_k \qquad \text{and} \qquad \mathcal{Q} = \bigcup_{k=1}^{K} \mathcal{Q}_k.$$

We then have

$$\begin{aligned} \#\mathcal{N}_2(p,K,H,h,w) &\ll h \sum_{m\in\mathcal{M}} \frac{1}{m} + \#\mathcal{M} \\ &\le \frac{h}{v!}\left(\sum_{q\in\mathcal{Q}} \frac{1}{q}\right)^v + \sum_{k=1}^{K} \binom{\omega(p^k-1)}{v}. \end{aligned}$$

Replacing the sum over primes in $\mathcal{Q}$ by the larger sum over the first $t = \#\mathcal{Q}$ primes, by the *Mertens theorem* (see, for example, Theorem 427 in [3]) we derive

$$\#\mathcal{N}_2(p,K,H,h,w) \ll \frac{h}{v!}\left(\log_2 t + O(1)\right)^v + \sum_{k=1}^{K} \frac{\omega(p^k-1)^v}{v!}.$$

As before, we remark that the inequality $\omega(p^k-1) \le k\log p$ holds for all sufficiently large values of the prime $p$, and thus the inequality $t \le K^2 \log p$

also holds for sufficiently large $p$. Applying the Stirling formula to $v!$, we finish the proof. □

LEMMA 2.4. *Let $H \ge h$, $\log H \asymp \log h \asymp \log p$ and $\log K = O(\log_2 p)$. Then the inequality*

$$\#\mathcal{N}(p, K, H, h) \le h^{1-1/(2\kappa+3)+o(1)}$$

*holds, where*

$$\kappa = \frac{\log K}{\log_2 p}.$$

*Proof.* Choosing

$$w = \left\lfloor \frac{2\log h}{2\log K + 2\log_2 p + \log_2 H} \right\rfloor,$$

to balance (asymptotically) the estimates of Lemmas 2.2 and 2.3, and taking into account that $\log H \asymp \log h$, we get that

$$\log\left(\frac{K \log H \log p}{w}\right) \sim \log K + \log_2 p.$$

We also remark that $\log_2 H \sim \log_2 h$. Therefore, noting that the hypotheses of Lemma 2.2 are satisfied, we get

$$\#\mathcal{N}_1(p, K, H, h, w) \le h^{\vartheta+o(1)},$$

where

$$\vartheta = \frac{2\log K + 2\log_2 p}{2\log K + 2\log_2 p + \log_2 H} = \frac{2\log K + 2\log_2 p}{2\log K + 3\log_2 p} + o(1) = \frac{2\kappa+2}{2\kappa+3} + o(1).$$

We also observe that

$$\log w \sim \log_2 h \sim \log_2 p.$$

Since $\log K = O(\log_2 p)$, we also have $\log_2(K^2 \log p) = w^{o(1)}$. Thus,

$$\begin{aligned}
\left(\frac{\log_2(K^2\log p)}{w}\right)^{w/2+o(w)} &= \exp(-(0.5+o(1))w\log w) \\
&= \exp\left(-(0.5+o(1))\frac{2\log h \log_2 p}{2\log K + 2\log_2 p + \log_2 H}\right) \\
&= h^{-1/(2\kappa+3)+o(1)}.
\end{aligned}$$

We also have

$$\begin{aligned}
K\left(\frac{C_2 K \log p}{w}\right)^{w/2} &= \exp\left((0.5+o(1))\, w \log K\right) \\
&= \exp\left((1+o(1))\,\frac{\log h \log K}{2\log K + 2\log_2 p + \log_2 H}\right) \\
&= h^{\kappa/(2\kappa+3)+o(1)} < h^{\vartheta+o(1)},
\end{aligned}$$

and the result follows. □

For real numbers $H \geq h \geq 1$ and any integer $K \geq 1$, we let $\mathcal{T}(p, K, H, h)$ be the set of positive integers $N$ in the interval $[H - h, H + h]$ and such that each prime divisor of $N$ divides $p^k - 1$ for some positive integer $k \leq K$; that is,

$$\mathrm{rad}(N) \,\Bigg|\, \prod_{k \leq K} (p^k - 1).$$

Accordingly, for an integer $w \geq 1$, let $\mathcal{T}_1(p, K, H, h, w)$ and $\mathcal{T}_2(p, K, H, h, w)$ be the subsets consisting of $N \in \mathcal{T}(p, K, H, h)$ with $\omega(N) \leq w$ and with $\omega(N) > w$, respectively. Using the same arguments as in the proofs of Lemmas 2.2 and 2.3, and remarking that

$$\omega\left(\prod_{k=1}^{K}(p^k - 1)\right) \leq K^2 \log p,$$

we obtain the following two results.

Lemma 2.5. *There exists a constant $C_3 > 0$ such that for any integer $w$ satisfying $w \to \infty$ in such a way that $w \leq 0.5K \log p$ the inequality*

$$\#\mathcal{T}_1(p, K, H, h, w) \ll \left(\frac{C_3 K^2 \log H \log p}{w}\right)^w$$

*holds.*

Lemma 2.6. *There exists a constant $C_4 > 0$ such that for any integer $w$ satisfying $w \to \infty$ and $H \geq h$ the inequality*

$$\#\mathcal{T}_2(p, K, H, h, w) \leq h\left(\frac{C_4 \log_2(K^2 \log p)}{w}\right)^{w/2} + \left(\frac{C_4 K^2 \log p}{w}\right)^{w/2}$$

*holds for large values of the prime $p$.*

In turn, a combination of Lemmas 2.5 and 2.6 leads to the following analogue of Lemma 2.7 .

Lemma 2.7. *Let $H \geq h$, $\log H \asymp \log h \asymp \log p$ and $\log K = O(\log_2 p)$. Then the inequality*

$$\#\mathcal{T}(p, K, H, h) \leq h^{1-1/(4\kappa+3)+o(1)}$$

*holds, where*

$$\kappa = \frac{\log K}{\log_2 p}.$$

*Proof.* Choosing

$$w = \left\lfloor \frac{2\log h}{4\log K + 2\log_2 p + \log_2 H} \right\rfloor,$$

to balance (asymptotically) the estimates of Lemmas 2.5 and 2.6, and taking into account that $\log H \asymp \log h$, we get that

$$\log\left(\frac{K^2 \log H \log p}{w}\right) \sim 2\log K + \log_2 p.$$

We also note that $\log_2 H \sim \log_2 h$. Therefore

$$\#\mathcal{T}_1(p, K, H, h, w) \le h^{\vartheta + o(1)},$$

where

$$\vartheta = \frac{4\log K + 2\log_2 p}{4\log K + 2\log_2 p + \log_2 H} = \frac{4\log K + 2\log_2 p}{4\log K + 3\log_2 p} + o(1) = \frac{4\kappa + 2}{4\kappa + 3} + o(1).$$

We also remark that

$$\log w \sim \log_2 h \sim \log_2 p.$$

Since $\log K = O(\log_2 p)$, we also have $\log_2(K^2 \log p) = w^{o(1)}$. Thus,

$$\begin{aligned}\left(\frac{\log_2(K^2\log p)}{w}\right)^{w/2+o(w)} &= \exp(-(0.5+o(1))w\log w)\\ &= \exp\left(-(0.5+o(1))\frac{2\log h \log_2 p}{4\log K + 2\log_2 p + \log_2 H}\right)\\ &= h^{-1/(4\kappa+3)+o(1)}.\end{aligned}$$

We also have

$$\begin{aligned}\left(\frac{C_4 K^2 \log p}{w}\right)^{w/2} &= \exp\left((0.5+o(1))\, w \log K\right)\\ &= \exp\left((1+o(1))\, \frac{\log h \log K}{4\log K + 2\log_2 p + \log_2 H}\right)\\ &= h^{\kappa/(4\kappa+3)+o(1)} < h^{\vartheta+o(1)},\end{aligned}$$

and the result follows. □

## 3. Main results

Theorem 3.1. *Let $p$ be a sufficiently large prime number, and let $K$ be a positive integer with $\log K = O(\log_2 p)$. Assume that $\mathbb{E}$ is a randomly chosen elliptic curve defined over $\mathbb{F}_p$. Let $N = \#\mathbb{E}(\mathbb{F}_p)$. The probability that $N \mid (p^k - 1)$ holds with some positive integer $k \le K$ is at most $p^{-1/(4\kappa+6)+o(1)}$, where*

$$\kappa = \frac{\log K}{\log_2 p}.$$

*Proof.* The result follows immediately from Lemma 2.1 and Lemma 2.4 applied with $H = p + 1$ and $h = 2p^{1/2}$. □

In particular, for $K = \lceil \log^2 p \rceil$, the probability estimate of Theorem 3.1 becomes $p^{-1/14+o(1)}$.

Clearly $R \mid L$, where $R = \mathrm{rad}\,(\#\mathbb{E}(\mathbb{F}_p))$ and $L$ is the exponent of $\mathbb{E}(\mathbb{F}_p)$. Accordingly, to estimate the probability of $L \mid (p^k - 1)$ for a small value of $k$, it is enough to estimate the probability that $R \mid (p^k - 1)$ for a small value of $k$.

Theorem 3.2. *Let $p$ be a sufficiently large prime number, and let $K$ be a positive integer with $\log K = O(\log_2 p)$. Assume that $\mathbb{E}$ is a randomly chosen elliptic curve defined over $\mathbb{F}_p$. Let $R = \mathrm{rad}\,(\#\mathbb{E}(\mathbb{F}_p))$. The probability that $R \mid (p^k - 1)$ holds with some positive integer $k \le K$ is at most $p^{-1/(4\kappa+6)+o(1)}$, where*

$$\kappa = \frac{\log K}{\log_2 p}.$$

*Proof.* For an integer $r \ge 1$ we let $S(p, K, r)$ be the number of integers $N \in \mathcal{I}_p$ such that $N = r^2 m$ with $m \mid (p^k - 1)$ for some positive integer $k \le K$. Clearly, for $r \ge 2p^{1/3}$ we have $m \le p^{1/3}$ provided $p$ is large enough. We also remark that for every $m \ge 1$ there are only $O(1)$ integer squares in the interval $[(p+1)/m - 2p^{1/2}/m, (p+1)/m + 2p^{1/2}/m]$, so

$$\sum_{r \ge 2p^{1/3}} S(p, K, r) \ll \sum_{m \le p^{1/3}} 1 \ll p^{1/3}.$$

We also have

$$\begin{aligned}\sum_{p^{1/6} \le r \le 2p^{1/3}} S(p, K, r) &\le \sum_{p^{1/6} \le r \le 2p^{1/3}} \left( \frac{4p^{1/2}}{r^2} + 1 \right) \\ &\le 4p^{1/2} \sum_{r \ge p^{1/6}} \frac{1}{r^2} + \sum_{p^{1/6} \le r \le 2p^{1/3}} 1 \ll p^{1/3}.\end{aligned}$$

For $r < p^{1/6}$ we use the obvious inequality

$$S(p, K, r) \le \#\mathcal{N}(p, K, (p+1)/r^2, 2p^{1/2}/r^2).$$

Therefore, by Lemma 2.4, we get

$$\sum_{r < p^{1/6}} S(p, K, r) \le \sum_{r < p^{1/6}} (p^{1/2}/r^2)^{1-1/(2\kappa+3)+o(1)} \le p^{1/2-1/(4\kappa+6)+o(1)}.$$

Applying Lemma 2.1, we finish the proof. □

In particular, for $K = \lceil \log^2 p \rceil$ the probability estimate of Theorem 3.2 becomes $p^{-1/14+o(1)}$.

It is certainly natural to combine MOV with the Pohling-Hellman type attack (see [2], [7]). More precisely, one can factor

$$N = \#\mathbb{E}(\mathbb{F}_p) = \prod_{i=1}^{s} p_i^{\alpha_i},$$

and then solve several discrete logarithm problems in the subgroups of $\mathbb{E}(\mathbb{F}_p)$ of orders $p_i$ for $i = 1, \ldots, s$. This brings up the question of whether prime divisors of $N$ are among the union of the prime divisors of $p^k - 1$, $k = 1, \ldots, K$, for some reasonably small $K$.

Accordingly, using Lemma 2.7 instead of Lemma 2.4 in the proof of Theorem 3.2, we obtain the following result.

Theorem 3.3. *Let $p$ be a sufficiently large prime number, and let $K$ be a positive integer with $\log K = O(\log_2 p)$. Assume that $\mathbb{E}$ is a randomly chosen elliptic curve defined over $\mathbb{F}_p$. Let $R = \mathrm{rad}\,(\#\mathbb{E}(\mathbb{F}_p))$. The probability that*

$$R \;\Bigg|\; \prod_{k \le K} (p^k - 1).$$

*is at most $p^{-1/(8\kappa+6)+o(1)}$, where*

$$\kappa = \frac{\log K}{\log_2 p}.$$

*Proof.* For an integer $r \ge 1$ we let $\widetilde{S}(p, K, r)$ be the number of integers $N \in \mathcal{I}_p$ such that $N = r^2 m$ with

$$m \;\Bigg|\; \prod_{k \le K} (p^k - 1).$$

As in the proof of Theorem 3.2, we derive

$$\sum_{r \ge p^{1/6}} \widetilde{S}(p, K, r) \ll p^{1/3} < p^{3/8}.$$

For $r < p^{1/6}$ we use the obvious inequality

$$\widetilde{S}(p, K, r) \le \#\mathcal{T}(p, K, (p+1)/r^2, 2p^{1/2}/r^2).$$

Therefore, by Lemma 2.7, we get

$$\sum_{r < p^{1/6}} \widetilde{S}(p, K, r) \le \sum_{r < p^{1/6}} (p^{1/2}/r^2)^{1-1/(4\kappa+3)+o(1)} \le p^{1/2-1/(8\kappa+6)+o(1)}.$$

Applying Lemma 2.1, we finish the proof. □

In particular, for $K = \lceil \log^2 p \rceil$ the probability estimate of Theorem 3.3 becomes $p^{-1/22+o(1)}$.

Theorem 3.4. *Let $p$ be a sufficiently large prime number, and let $K$ be a positive integer with $\log K = O(\log_2 p)$. Assume that $\mathbb{E}$ is a randomly chosen elliptic curve defined over $\mathbb{F}_p$. Let $Q = P\left(\#\mathbb{E}(\mathbb{F}_p)\right)$. The probability that $Q \mid (p^k - 1)$ holds with some positive integer $k \le K$ is at most $\exp\left(-0.2(\log p \log_2 p)^{1/2}\right)$, provided that $p$ is large enough.*

*Proof.* Let $u \ge 1$ be a real number and let

$$y = p^{1/2u}.$$

It follows, by known results on smooth numbers in short intervals (see, for example, [4]), that for $u \to \infty$ the number of values of $N \in \mathcal{I}_p$ such that $P(N) \le y$ is at most $p^{1/2} \exp\left(-(1 + o(1))u \log u\right)$.

On the other hand, the number of values of $N$ satisfying both $P(N) > y$ and $P(N) \mid (p^k - 1)$ with some positive integer $k \le K$, is at most

$$\sum_{k=1}^{K} \omega(p^k - 1) \left(\frac{4p^{1/2}}{y} + 1\right) \ll p^{1/2} y^{-1} K^2 \log p.$$

Thus, the total number of $N \in \mathcal{I}_p$ such that $P(N) \mid (p^k - 1)$ holds with some positive integer $k \le K$ is $O\left(p^{1/2}\left(\exp\left(-(1 + o(1))u \log u\right) + y^{-1} K^2 \log p\right)\right)$.

Choosing

$$u = \left(\frac{\log p}{5 \log_2 p}\right)^{1/2},$$

we see that the inequality

$$u \le \frac{\log p}{8 \log K}$$

holds provided that $p$ is large enough. Therefore, we obtain that the inequality

$$\exp\left(-(1 + o(1))u \log u\right) \ge p^{-1/4u} \ge p^{-1/2u} K^2 = y^{-1} K^2$$

holds for sufficiently large $p$. Applying Lemma 2.1, after simple calculations, we finish the proof. □

In particular, the probability estimate of Theorem 3.4 applies for $K = \lceil \log^2 p \rceil$.

It is easy to see that one can improve the constant 0.2 in the exponents of the bound of Theorem 3.4.

Our techniques may also be employed to produce nontrivial bounds on the above probabilities in a much wider range than $\log K = O(\log_2 p)$ requested in our results. We choose not to detail these bounds here as the formulations become more complicated.

## References

[1] R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptology **11** (1998), 141–145. MR 2000f:94024

[2] R. Crandall and C. Pomerance, *Prime numbers*, Springer-Verlag, New York, 2001. MR 2002a:11007

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, The Clarendon Press Oxford University Press, New York, 1979. MR 81i:10002

[4] A. Hildebrand, *Integers free of large prime divisors in short intervals*, Quart. J. Math. Oxford Ser. (2) **36** (1985), 57–69. MR 86f:11066

[5] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673. MR 89g:11125

[6] A. J. Menezes, T. Okamoto, and S. A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inform. Theory **39** (1993), 1639–1646. MR 95e:94038

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997. MR 99g:94015

[8] O. Schirokauer, *Discrete logarithms and local units*, Philos. Trans. Roy. Soc. London Ser. A **345** (1993), 409–423. MR 95c:11156

[9] O. Schirokauer, D. Weber, and T. Denny, *Discrete logarithms: the effectiveness of the index calculus method*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 337–361. MR 98i:11109

Florian Luca, Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58180, Morelia, Michoacán, Mexico

*E-mail address*: `fluca@matmor.unam.mx`

David Jose Mireles, Facultad de Ciencias, Universidad Nacional Autónoma de México, C.P. 04510, Ciudad Universitaria, México D.F., Mexico

*E-mail address*: `davo@ciencias.unam.mx`

Igor E. Shparlinski, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

*E-mail address*: `igor@ics.mq.edu.au`