

## On Primitive Roots Conjecture for Certain Two-Dimensional Tori

04/24/00

Yen-Mei J. Chen and Jing Yu

Dept. of Math., Tamkang University, Tamshui, Taipei, Taiwan

Institute of Math., Academia Sinica, Nankang, Taipei, Taiwan

and National Center for Theoretical Sciences, Hsinchu, Taiwan

E-mail: ymjchen@mail.tku.edu.tw

E-mail: yu@math.sinica.edu.tw

We prove an analogue of Artin's primitive roots conjecture for 2-dimensional tori  $\text{Res}_{K/\mathbb{Q}} \mathbb{G}_m$  under Generalized Riemann Hypothesis, where  $K$  are imaginary quadratic fields. As a consequence, we are able to derive a precise density formula for a given non-supersingular elliptic curves over a finite field which tells how often the Galois extension of the base field obtained by adjoining all coordinates of  $\ell$ -torsion has degree  $\ell^2 - 1$  as  $\ell$  running through rational primes. It turns out the density in question is essentially independent of the curves, even independent of the characteristic  $p$  if  $p \not\equiv 1 \pmod{4}$ .

### §1.

Given an elliptic curve  $E/\mathbb{F}_p$ , we are interested in the Galois representations on  $\ell$ -torsion  $E[\ell] \subset E(\mathbb{F}_p)$  for various rational prime numbers  $\ell$ . Let  $\mathbb{F}_p(E[\ell])$  be the Galois extension of  $\mathbb{F}_p$  obtained by adjoining all coordinates of points in  $E[\ell]$ . A basic question is: how often the degree  $[\mathbb{F}_p(E[\ell]) : \mathbb{F}_p]$  can be the largest possible, in other words, is equal to  $\ell^2 - 1$ ?

If the given curve  $E/\mathbb{F}_p$  is supersingular, one can deduce easily that for almost all  $\ell$ , the degree of  $\mathbb{F}_p(E[\ell])/\mathbb{F}_p$  is  $\leq 2(\ell - 1)$ . Thus for our purpose it suffices to consider non-supersingular elliptic curves. We study the following set associated to a given non-supersingular  $E/\mathbb{F}_p$ :

$$M_E = \{\ell \mid \ell \text{ prime, } [\mathbb{F}_p(E[\ell]) : \mathbb{F}_p] = \ell^2 - 1\}.$$

The result we obtain is that, under generalized Riemann Hypothesis (GRH), these sets  $M_E$  always have positive density. Furthermore the value of this density  $\text{den}(M_E)$  can be given precisely in terms of a universal constant  $C_2$ :

$$C_2 = \frac{1}{4} \prod_{q \neq 2} \left(1 - \frac{2}{q(q-1)}\right) = 0.133776\dots,$$

If  $p \not\equiv 1 \pmod{4}$ , then always  $\text{den}(M_E) = C_2$ . On the other hand, if  $p \equiv 1 \pmod{4}$ , then  $\text{den}(M_E) = (1 - \frac{2}{p(p-1)})^{-1}C_2$  unless in certain exceptional cases where  $\text{den}(M_E)$  are still equal to  $C_2$  (c.f. Theorem 4.3).

Our approach is based on a variation of Artin's primitive roots problem for a family of two-dimensional tori over  $\mathbb{Q}$ . Let  $\text{End}_E$  denote the endomorphism ring of the elliptic curve  $E$  and let  $\alpha \in \text{End}_E$  be the Frobenius endomorphism. If  $E$  is not supersingular,  $\mathbb{Z}[\alpha] \subset \text{End}_E$  is identified with an order in an imaginary quadratic field  $K = K_E$ . Then  $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ , the ring of integers in  $K$ . The torus in question is the one obtained from  $\mathbb{G}_{m/K}$  via restriction of scalars:  $\mathbb{T} = \text{Res}_{K/\mathbb{Q}} \mathbb{G}_{m/K}$ . We have  $\alpha \in K^* = \mathbb{T}(\mathbb{Q})$  non-torsion and what we are searching are the rational primes  $\ell$  which stay prime in  $K$  and  $\alpha$  modulo  $\ell$  is primitive, i.e.  $\alpha$  modulo  $\ell$  is a generator of the cyclic group  $(\mathcal{O}_K/\ell\mathcal{O}_K)^*$ .

## §2.

Let  $K$  be a fixed imaginary quadratic number field, with ring of integers  $\mathcal{O}_K \subset K$ . We use  $\tau$  to denote complex conjugation and  $\ell$  always stands for a rational prime number which stay prime in  $K$ . For  $\alpha \neq 0 \in \mathcal{O}_K$ ,  $N(\alpha) = \alpha\alpha^\tau$  denotes its absolute norm,  $\bar{\alpha}$  denotes the coset in  $(\mathcal{O}_K/\ell\mathcal{O}_K)^*$  containing  $\alpha$  if  $\text{ord}_\ell(\alpha) = 0 = \text{ord}_\ell(1/\alpha)$ , and  $o_\ell(\alpha)$  denotes the order of  $\bar{\alpha}$  inside  $(\mathcal{O}_K/\ell\mathcal{O}_K)^*$ . The set of all rational prime numbers is denoted by  $\mathbb{P}$ . Given  $\alpha \in \mathcal{O}_K^*$ , we set  $u = u(\alpha) = \alpha^\tau/\alpha$ . Our starting point is:

**Proposition 2.1.** *Let  $\ell \in \mathbb{P}$  be a prime which is inert(stays prime) in  $K$  and  $\ell \nmid \alpha$ . Then  $o_\ell(\alpha) = \ell^2 - 1$  if and only if  $o_\ell(N(\alpha)) = \ell - 1$  and  $o_\ell(u) = \ell + 1$ .*

Consider

$$\begin{aligned} M_\alpha &= \{\ell \in \mathbb{P} : \ell \text{ is inert in } K, \ell \nmid \alpha, o_\ell(\alpha) = \ell^2 - 1\} \\ &= \{\ell \in \mathbb{P} : \ell \text{ is inert in } K, \bar{\alpha} \text{ generate } \mathbb{T}(\mathbb{F}_\ell)\}. \end{aligned}$$

**Notations:** Let  $q, q'$  denote elements of  $\mathbb{P}$  with  $q'$  odd. We set

$$F_1 = K, E_1 = \mathbb{Q}.$$

$$\mu_q = \text{the group of } q\text{-th roots of unity.}$$

$$E_q = \mathbb{Q}(\mu_q, \sqrt[q]{N(\alpha)}).$$

$$E_m = \prod_{q|m} E_q, \text{ for square free } m.$$

$$F_{q'} = K(\mu_{q'}, \sqrt[q']{u}).$$

$$F_n = \prod_{q'|n} F_{q'}, \text{ for square free odd } n.$$

$$L_{mn} = E_m F_n \text{ for } m, n \text{ square free and } n \text{ is odd.}$$

$$G_{mn} = \text{Gal}(L_{mn}/\mathbb{Q}).$$

$$d_{mn} = \#G_{mn}.$$

$$C_{mn} = \{\sigma \in G_{mn} : \sigma|_K = \tau, \sigma|_{E_m} = \text{id}, \sigma|_{\mathbb{Q}(\mu_n)} = \tau, \text{ and } \sigma^2 = \text{id}\}.$$

$$c_{nn} = \#C_{mn}.$$

$(\ell, E/\mathbb{Q})$  denotes Artin symbol, where  $E/\mathbb{Q}$  is finite Galois extension.

The following Proposition is crucial:

**Proposition 2.2.** *Let  $\ell$  be a rational prime which is inert in  $K/\mathbb{Q}$  and  $\ell \nmid \alpha$ . Then  $\ell \in M_\alpha$  if and only if  $(\ell, L_{q1}/\mathbb{Q}) \not\subseteq C_{q1}$  for all prime  $q$  and  $(\ell, L_{1q'}/\mathbb{Q}) \not\subseteq C_{1q'}$  for all odd prime  $q'$ .*

A detailed study of the Galois family  $L_{mn}$ , together with computation of  $c_{mn}$ , is needed. We have the following technical lemmas.

**Lemma 2.3.** *Let  $m, n$  be square-free positive integers with  $n$  odd. Let  $s$  be the largest integer with the property that  $N(\alpha) \in (\mathbb{Q}^*)^s$  (then  $(\alpha) = \mathfrak{a}^s$  for some ideal  $\mathfrak{a}$  in  $\mathcal{O}_K$ ). Let  $m_1 = m/\gcd(s, m)$  and  $n_2 = n/\gcd(\frac{s}{o}, n)$  where  $o$  is the order of  $\mathfrak{a}$  in the ideal class group of  $K$ . Suppose  $\gcd(\alpha, \alpha^\tau) = 1$  and  $\gcd(s, 6) = 1$ . Then*

(a)

$$[E_m : \mathbb{Q}] = \frac{m_1 \phi(m)}{[k_m \cap \mathbb{Q}(\mu_m) : \mathbb{Q}]},$$

where  $k_m = \mathbb{Q}$  (resp.  $\mathbb{Q}(\sqrt{N(\alpha)})$ ) if  $2 \nmid m$  (resp.  $2 \mid m$ ).

(b)

$$[F_n : \mathbb{Q}] = \begin{cases} \frac{2n_2 \phi(n)}{3[K \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{if } K = \mathbb{Q}(\sqrt{-3}), 3 \mid n, \text{ and } u \in (K(\mu_n)^*)^3, \\ \frac{2n_2 \phi(n)}{[K \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]} & \text{othersiwe.} \end{cases}$$

**Lemma 2.4.** *Let  $m, n$  be square-free positive integers with  $n$  odd and  $\gcd(m, n) = 1$ . Suppose further that  $\alpha$  satisfies all the conditions in Lemma 2.3. If  $K = \mathbb{Q}(\sqrt{-3})$ ,  $3 \mid n$  and  $u \in (K(\mu_{mn})^*)^3 - (K(\mu_n)^*)^3$ , then  $E_m \cap F_n = k_m(\mu_m) \cap K(\mu_n, \sqrt[3]{u})$  and*

$$[E_m \cap F_n : \mathbb{Q}] = \frac{3[Kk_m \cap \mathbb{Q}(\mu_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\mu_m) : \mathbb{Q}][K \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]}.$$

Otherwise,  $E_m \cap F_n = k_m(\mu_m) \cap K(\mu_n)$  and

$$[E_m \cap F_n : \mathbb{Q}] = \frac{[Kk_m \cap \mathbb{Q}(\mu_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\mu_m) : \mathbb{Q}][K \cap \mathbb{Q}(\mu_n) : \mathbb{Q}]}.$$

**Lemma 2.5.** *Let  $m, n$  be square-free positive integers with  $n$  odd. Suppose further that  $\alpha$  satisfies all the conditions in Lemma 2.3. Then*

$$c_{mn} = \begin{cases} 1 & \text{if } \gcd(m, n) = 1 \text{ and } E_m \cap F_n \text{ is totally real,} \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 2.6.** *Let  $m, n$  be square-free positive integers with  $n$  odd and  $\gcd(m, n) = 1$ . Suppose further that  $\alpha$  satisfies all the conditions in Lemma 2.3. Then*

$$d_{mn} = \begin{cases} \frac{2m_1 n_2 \phi(mn)}{3[Kk_m \cap \mathbb{Q}(\mu_{mn}) : \mathbb{Q}]} & \text{if } K = \mathbb{Q}(\sqrt{-3}), 3 \mid n, \text{ and } u \in (K(\mu_{mn})^*)^3, \\ \frac{2m_1 n_2 \phi(mn)}{[Kk_m \cap \mathbb{Q}(\mu_{mn}) : \mathbb{Q}]} & \text{othersiwe.} \end{cases}$$

### §3.

The existence of density for  $M_\alpha$  is contained in the following

**Theorem 3.1.** *Given  $\alpha \neq 0 \in \mathcal{O}_K$  with  $\gcd(\alpha, \alpha^\tau) = 1$ . Let  $s$  be the largest integer such that  $N(\alpha) \in (\mathbb{Q}^*)^s$ . Assume that  $\gcd(s, 6) = 1$  and furthermore GRH holds. Then  $\text{den}(M_\alpha)$  exists and is given by*

$$\text{den}(M_\alpha) = \sum_{m, n} \frac{\mu(m)\mu(n)c_{mn}}{d_{mn}},$$

where in the sum  $m, n$  runs through all square free positive integers,  $n$  is required to be odd.

The proof of the above Theorem is based on analytic method originated from Hooley [3], which uses effective Chebotarev Density Theorem and assumes GRH. For the detail of the proof, we refer to [2].

We are particularly interested in the case  $N(\alpha) = p^s$ , where  $p$  is a prime splitting in the imaginary quadratic field  $K$ . The case  $K = \mathbb{Q}(\sqrt{-3}) = K(\mu_3)$  requires special attention. Suppose that  $K = \mathbb{Q}(\sqrt{-3})$  and  $\alpha \neq 0 \in \mathcal{O}_K$ ,  $\gcd(\alpha, \alpha^\tau) = 1$ , and  $N(\alpha) = p^s$ , with  $s$  an integer prime to 6. Then the principal ideal  $(\alpha)$  is equal to  $(\beta)^s$  for some primary prime of  $\mathcal{O}_K$  lying above  $p$ . There is a unique integer  $\delta(\alpha)$  modulo 6 with  $\alpha = \zeta_6^{\delta(\alpha)} \beta^s$ . From the classical theory of cubic Gauss sums (c.f. [4], Chap. 9), one knows that  $p\beta \in K(\mu_p)^{*3}$ . Then it follows that for any square-free odd integer  $n$ ,  $u = \frac{\alpha^\tau}{\alpha} \in K(\mu_n)^{*3}$  if and only if  $3 \mid \delta(\alpha)$  and  $p \mid n$ . We call an imaginary quadratic integer  $\alpha$  exceptional if  $\alpha \in K$ , and  $\alpha = \pm\beta^s$  with  $\beta$  primary prime. All other imaginary quadratic integers are called nonexceptional.

Let  $h$  denotes the class number of  $K$ . For any positive integer  $c$ , define  $f(c) = \#\{q \in \mathbb{P} : q \mid c, q \text{ is odd.}\}$ . Our main theorem is

**Theorem 3.2.** *Assume GRH holds. Suppose  $\alpha \neq 0 \in \mathcal{O}_K$ ,  $\gcd(\alpha, \alpha^\tau) = 1$  and  $N(\alpha) = p^s$ , where  $p$  is a prime splitting in  $K$ ,  $s$  is an integer satisfying  $\gcd(6, s) = 1$  and  $f(s) = f(\frac{s}{\gcd(s, h)})$ . Then  $M_\alpha$  has positive density given by*

$$\text{den}(M_\alpha) = \begin{cases} \frac{1}{4} \prod_{q \mid s, q \neq p} \left(1 - \frac{2}{(q-1)}\right) \prod_{q \geq 3, q \nmid ps} \left(1 - \frac{2}{q(q-1)}\right) & \text{if } p \equiv 1 \pmod{4} \text{ and } \alpha \\ & \text{nonexceptional} \\ \frac{1}{4} \prod_{q \mid s} \left(1 - \frac{2}{(q-1)}\right) \prod_{q \geq 3, q \nmid s} \left(1 - \frac{2}{q(q-1)}\right) & \text{otherwise.} \end{cases}$$

The proof is divided into various cases according to  $K = \mathbb{Q}(\sqrt{-3})$  or  $K \neq \mathbb{Q}(\sqrt{-3})$ , according to  $p \pmod{4}$ , as well as the discriminant  $D_K \pmod{8}$ . We refer to [2] for details. Here we shall present only one simple case: suppose that  $p \equiv 1 \pmod{4}$  and  $D_K \equiv 0 \pmod{4}$ .

By Lemma 2.4 for relatively prime square free positive integer  $m, n$  with  $n$  odd, we have

$$E_m \cap F_n = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } 2 \mid m \text{ and } p \mid n, \\ \mathbb{Q} & \text{otherwise,} \end{cases}$$

Then from Lemma 2.5 and 2.6, we obtain

$$c_{mn} = 1 \text{ and } d_{mn} = \begin{cases} m_1 n_1 \phi(mn) & \text{if } 2p \mid mn, \\ 2m_1 n_1 \phi(mn) & \text{otherwise.} \end{cases}$$

Applying Theorem 3.1, we have

$$\begin{aligned} \text{den}(M_\alpha) &= \sum_{\substack{m, n \\ 2p \nmid mn}} \frac{\mu(mn)}{2m_1 n_1 \phi(mn)} + \sum_{\substack{m, n \\ 2p \mid mn}} \frac{\mu(mn)}{m_1 n_1 \phi(mn)} \\ &= \sum_{2p \nmid c} \frac{2^{f(c)} \mu(c)}{2c_1 \phi(c)} + \sum_{2p \mid c} \frac{2^{f(c)} \mu(c)}{c_1 \phi(c)} \\ &= \sum_c \frac{2^{f(c)} \mu(c)}{2c_1 \phi(c)} + \sum_{2p \mid c} \frac{2^{f(c)} \mu(c)}{2c_1 \phi(c)} \\ &= \frac{1}{4} \prod_{q \geq 3} \left(1 - \frac{2}{q_1(q-1)}\right) + \frac{1}{2p_1(p-1)} \prod_{q \geq 3, q \neq p} \left(1 - \frac{2}{q_1(q-1)}\right) \\ &= \frac{1}{4} \prod_{q \geq 3, q \neq p} \left(1 - \frac{2}{q_1(q-1)}\right) \\ &= \frac{1}{4} \prod_{q \mid s, q \neq p} \left(1 - \frac{2}{(q-1)}\right) \prod_{q \geq 3, q \nmid ps} \left(1 - \frac{2}{q(q-1)}\right) > 0. \end{aligned}$$

§4. Let  $\mathbb{F}_r$  denote a finite field of characteristic  $p$  with  $r = p^s$  elements. Given an elliptic curve  $E$  defined over  $\mathbb{F}_r$ , we would like to know the size of the Galois extension of  $\mathbb{F}_r$  obtained through adjoining all coordinates of  $\ell$ -torsion points where  $\ell$  is a prime. The size in question is the degree  $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$  which equals to the order of the Frobenius endomorphism acting on  $E[\ell]$ . If the curve  $E$  is not supersingular, it is well-known that  $\mathbb{Z}[\alpha] \subset \text{End}_E$  which can be identified with an order in an imaginary quadratic field  $K = K_E$ . If  $E$  is supersingular, it may happen that  $\alpha_E \in \mathbb{Z}$ , or else  $\mathbb{Z}[\alpha]$  is still contained in an imaginary quadratic field  $K = K_E$ . We let  $\text{disc}(\alpha)$  be the discriminant of  $\mathbb{Z}[\alpha]$ . The following proposition bounds  $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$  in the non supersingular case:

**Proposition 4.1.** *Given non-supersingular elliptic curve  $E/\mathbb{F}_r$  with (geometric) Frobenius endomorphism  $\alpha$  in imaginary quadratic field  $K$ . Let  $e_2$  be the largest divisor of 24 such that  $\alpha \in (K^*)^{e_2}$ , and  $e_1 = 2$ , or 1 according as whether  $\alpha$  is a square in  $K$ . Suppose prime  $\ell > 3$  and  $\ell \nmid p \text{ disc}(\alpha)$ . Then*

$$[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] \leq \begin{cases} \frac{\ell^2 - 1}{e_2}, & \text{if } \ell \text{ is inert in } K/\mathbb{Q} \\ \frac{\ell - 1}{e_1}, & \text{if } \ell \text{ splits in } K/\mathbb{Q} \end{cases}$$

We are interested in the distribution of the degrees  $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$  as the prime number  $\ell$  varies. In particular, how often the Galois extension degree  $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$  can be the largest possible, in other words, is equal to  $(\ell^2 - 1)/e_2$ ? We consider therefore the following set of primes :

$$M_E = \{\ell \mid \ell \in \mathbb{P}, [\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] = (\ell^2 - 1)/e_2\}.$$

We have

**Theorem 4.2.** *Assume GRH holds, and suppose  $\gcd(s, 6) = 1$ . Let  $E/\mathbb{F}_r$  be any elliptic curve which is not supersingular. Then the set  $M_E$  always has positive density.*

*Proof.* Let  $K = K_E$ , with  $h$  equals to the class number of  $\mathcal{O}_K$ . First, we apply Theorem 3.1 to the Frobenius  $\alpha = \alpha_E$ . This shows that the set  $M_E$  has a density, since it differs from  $M_\alpha$  only by a finite set. Next we can multiply  $s$  by suitable powers of those prime factors of  $h$  not dividing 6 so that  $s'$  and  $s'/\gcd(s', h)$  has the same set of odd prime factors. Extending the base field to  $\mathbb{F}_{p^{s'}}$ , and replacing the given curve  $E$  by  $E'/\mathbb{F}_{p^{s'}}$ . Then the Frobenius  $\alpha' = \alpha_{E'}$  satisfies the hypothesis of Theorem 3.2. It follows that the set  $M_{E'}$  has positive density. To finish the proof, it suffices to show that  $M_{\alpha'} \subseteq M_\alpha$ . This follows from the fact that the order of  $\alpha$  modulo  $\ell$  is at least the order of  $\alpha'$  modulo  $\ell$  because  $\alpha'$  is a power of  $\alpha$ .  $\square$

For prime fields  $\mathbb{F}_r = \mathbb{F}_p$ , precise value of the density can be given. Since  $\text{den}(M_E) = \text{den}(M_\alpha)$  in this case ( $s=1$ ), the desired formula follows from Theorem 3.2 immediately.

**Theorem 4.3.** *Given elliptic curve  $E/\mathbb{F}_p$  which is not supersingular. Suppose GRH holds. Then the density of  $M_E$  is :*

$$\text{den}(M_E) = \begin{cases} \left(1 - \frac{2}{p(p-1)}\right)^{-1} C_2 & \text{if } p \equiv 1 \pmod{4} \text{ and } \alpha \\ & \text{nonexceptional} \\ C_2 & \text{otherwise,} \end{cases}$$

If the curve  $E$  is supersingular, bounds on  $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$  is

**Proposition 4.4.** Suppose  $E/\mathbb{F}_r$  is supersingular and  $\ell$  does not divide  $\text{disc}(\alpha)$ . Then

$$[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] \leq \begin{cases} (\ell - 1), & \text{if } t_E = \pm 2\sqrt{r}, \text{ and } s \text{ even} \\ 2(\ell - 1), & \text{if } t_E = 0 \\ 3(\ell - 1), & \text{if } t_E = \pm\sqrt{r}, \text{ and } s \text{ even} \\ 4(\ell - 1), & \text{if } t_E = \pm p^{(s+1)/2}, s \text{ odd, and } p = 2 \\ 6(\ell - 1), & \text{if } t_E = \pm p^{(s+1)/2}, s \text{ odd, and } p = 3 \end{cases}$$

where  $t_E \in \mathbb{Z}$  is the trace of the Frobenius endomorphism.

We obtain therefore the following characterization of supersingular elliptic curves:

**Corollary 4.5.** Assume GRH holds. Then  $E/\mathbb{F}_p$  is supersingular if and only if  $[\mathbb{F}_p(E[\ell]) : \mathbb{F}_p] = O(\ell - 1)$  as  $\ell$  runs through the rational primes.

### References

- [1] Y.-M. J. Chen, Y. Kitaoka, and J. Yu, *Distributions of units of real quadratic number fields*, Nagoya Math. J., to appear.
- [2] Y.-M. J. Chen, and J. Yu, *On a density problem for elliptic curves over finite fields*, Preprint, 2000.
- [3] C. Hooley, *On Artin's conjecture*, J. reine angew Math. 225(1967), 209-220.
- [4] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York 1982.
- [5] H.W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Inventiones math. 42, 201-224(1977).
- [6] M.R. Murty, *On Artin's conjecture*, Journal of Number Theory 16, 147-168(1983).
- [7] J.-P. Serre, *Quelques applications du Théorème de densité de Chebotarev*, Publ. Math. IHES, 54(1981), 123-201.
- [8] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. scient. EC. Norm. Sup., 2(1969), 521-560.