Pseudorandom Number Generators Based on Elliptic Curves

Tanja Lange

Ruhr-University Bochum

Germany

Igor Shparlinski

Macquarie University

Australia

Overview

- Motivation
- (Brief) introduction to elliptic curves
- Discrepancy
- PRNGs from elliptic curves
  - Linear congruential generator
  - EC Power generator
  - Naor-Reingold generator
- Bounds for the power generator
- Koblitz curves

Motivation

- Nice proposal of PRNG
- Study helps to increase trust in EC-DLP
  bad performance with respect to some measure could be turned into attack.
  Some PRNGs related to

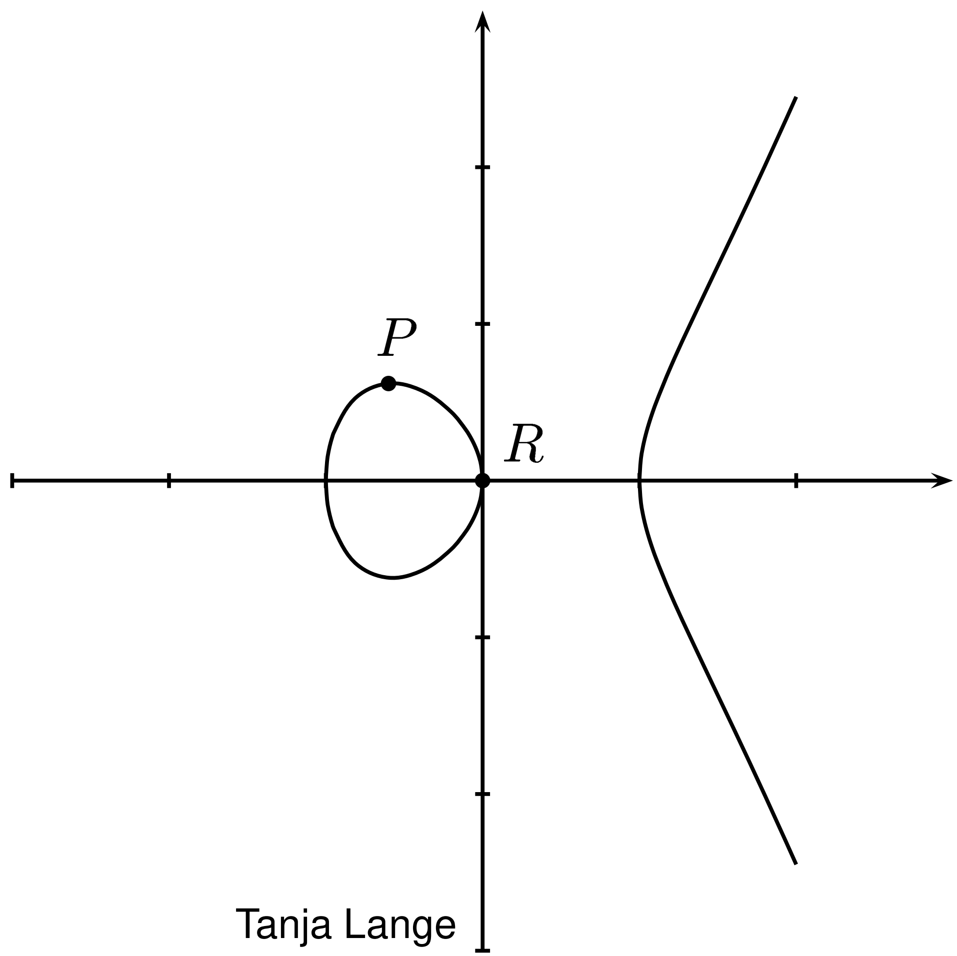
  Discrete Logarithm Problem (DLP)

  Given P and $Q = kP$ find k!
- Nice application of character sums and curves :–)

Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

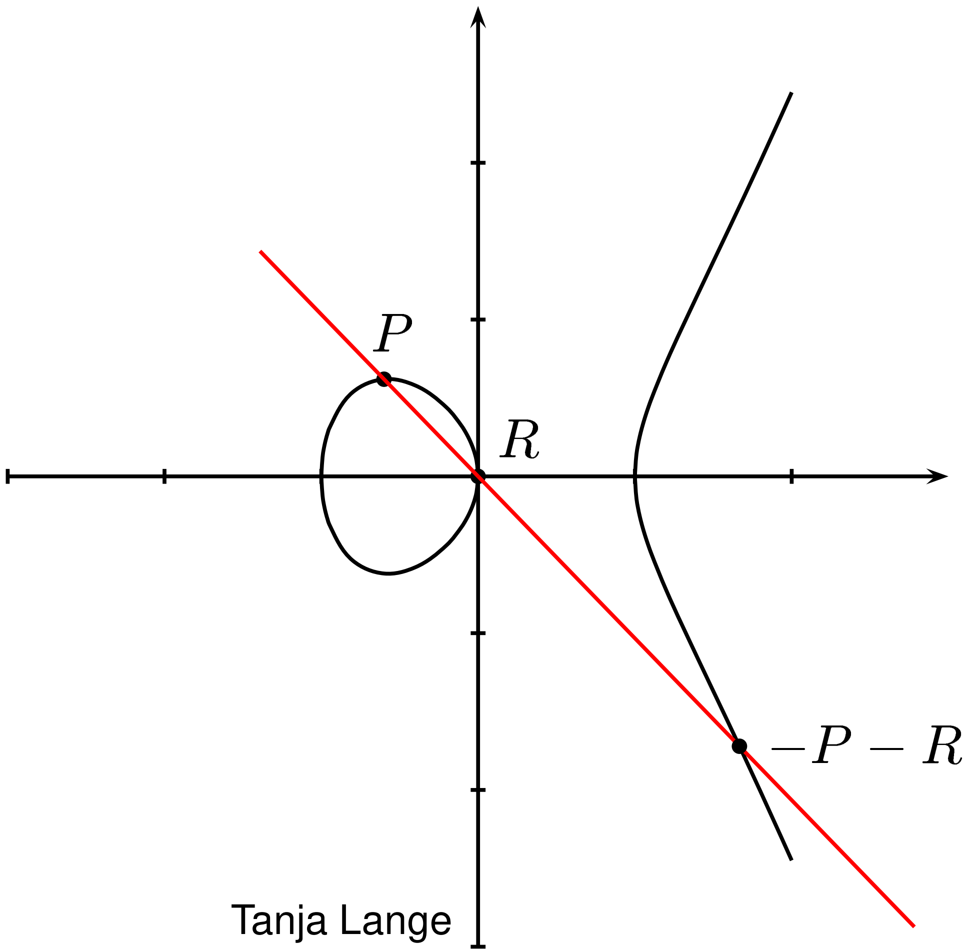


over $\mathbb{R}$

Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$

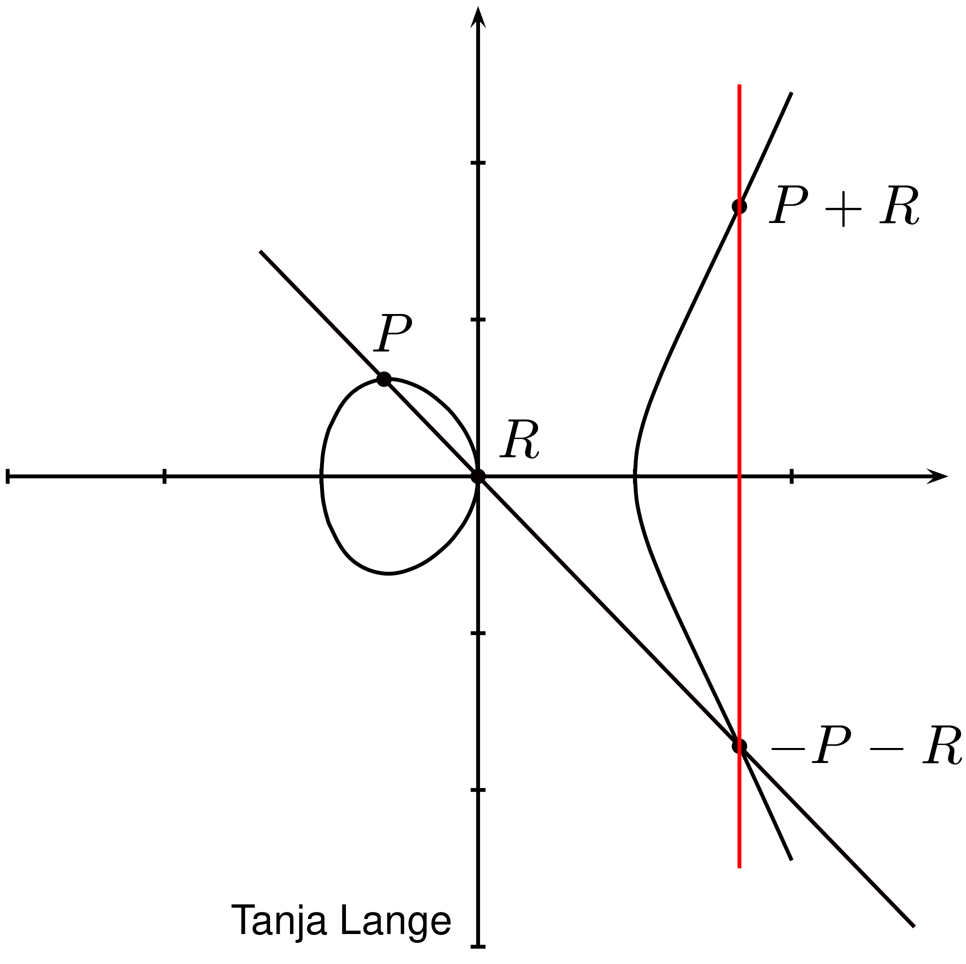


over $\mathbb{R}$

Elliptic Curve

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)}\, y = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \;\; h, f \in \mathbb{F}_q[x]$$

Group: $E(\mathbb{F}_q) = \{\, (x, y) \in \mathbb{F}_q^2 \,:\, y^2 + h(x)y = f(x)\,\} \cup \{\, P_\infty \,\}$

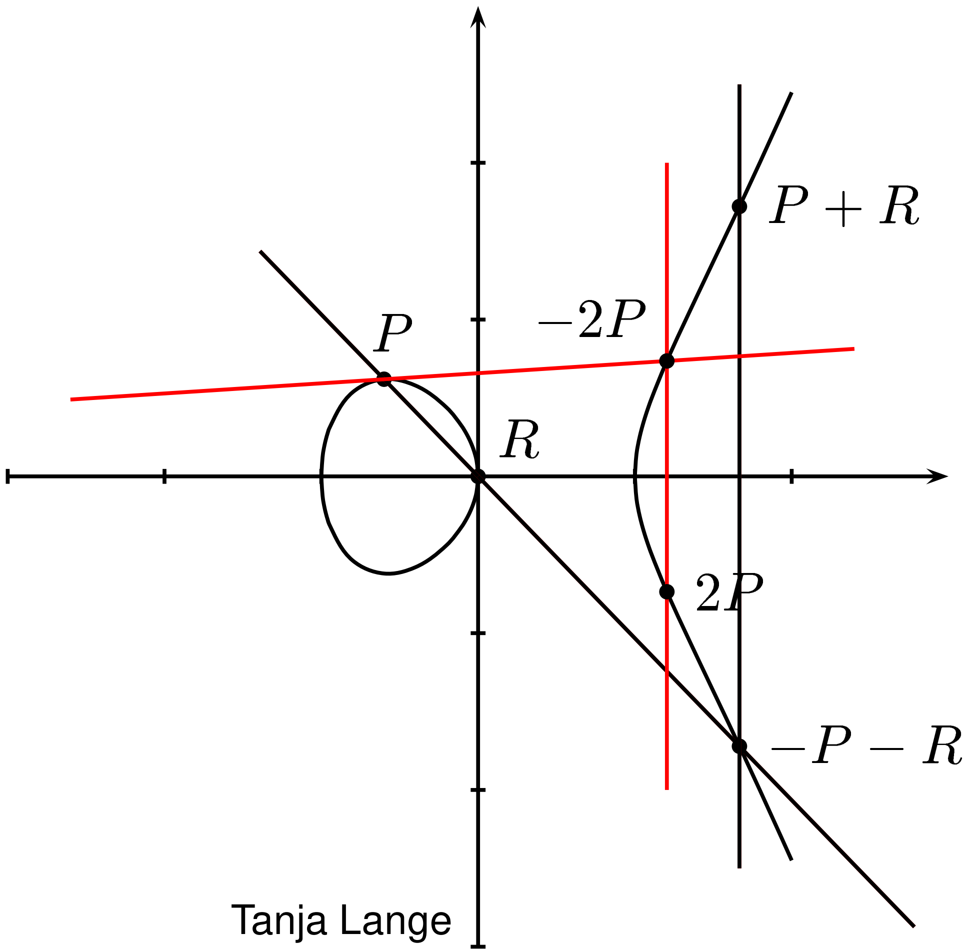


over $\mathbb{R}$

Elliptic Curve

$$E : y^2 + \underbrace{(a_1 x + a_3)}_{h(x)} y = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{f(x)}, \quad h, f \in \mathbb{F}_q[x]$$

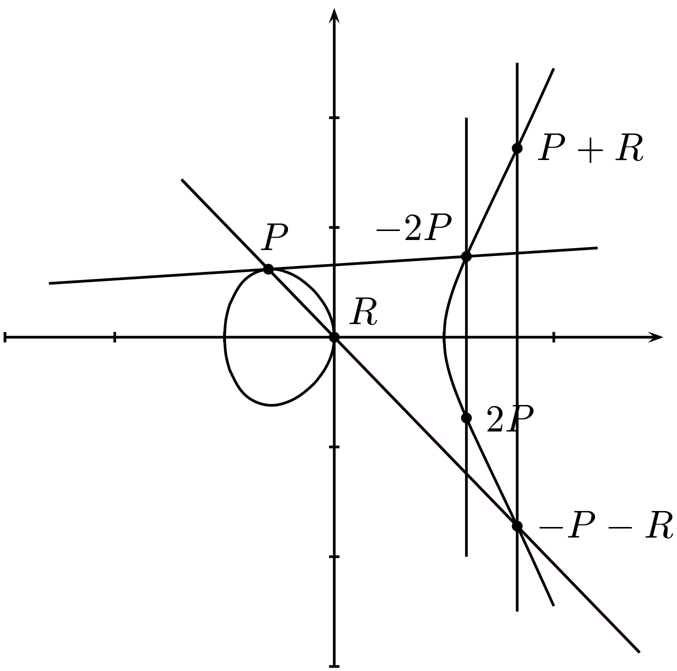
Group: $E(\mathbb{F}_q) = \{ (x, y) \in \mathbb{F}_q^2 : y^2 + h(x)y = f(x) \} \cup \{ P_\infty \}$



over $\mathbb{R}$

Group Law (q odd)

$$E : y^2 = x^3 + a_4x + a_6, \; a_i \in \mathbb{F}_q$$



$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= \\ &= (x_3, y_3) = \\ &= (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1),\end{aligned}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } x_1 \neq x_2, \\ (3x_1^2 + a_4)/(2y_1) & \text{else.} \end{cases}$$

$\Rightarrow$ consider sequence of points $P_n \in E(\mathbb{F}_q)$.

Let $P \in E(\mathbb{F}_q)$ be a point of order ℓ, often ℓ is assumed to be a prime.

Discrepancy - general

For a sequence of N points in the unit cube $[0,1) \times [0,1)$

$$\Gamma = \{(\gamma_{1,n}, \gamma_{2,n}) \in [0,1) \times [0,1), \quad 1 \leq n \leq N\}$$

its *discrepancy* $\Delta(\Gamma)$ is

$$\Delta(\Gamma) = \sup_{B \subseteq [0,1)^2} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of Γ which hit the box

$$B = [\alpha_1, \beta_1) \times [\alpha_2, \beta_2) \subseteq [0,1) \times [0,1)$$

and the supremum is taken over all such boxes.

Sequences from points

Map points $P_n = (x_n, y_n) \in \mathbb{F}_q^2$ into $[0,1) \times [0,1)$ and request that the discrepancy is small.
If $q = p$ prime then there is a natural map

$$P_n \to \left(\frac{x_n}{p}, \frac{y_n}{p}\right)$$

(think $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$).

Some applications use only x-coordinate.

Elliptic curve PRNGs I

- EC Linear Congruential Generator, **EC-LCG**:
  For the "initial value" $Q_0 \in E(\mathbb{F}_q)$, consider the sequence:

  $$Q_k = P \oplus Q_{k-1} = kP \oplus Q_0, \qquad k = 1, 2, \ldots .$$

  Easy to construct following element given two consecutive ones.

- EC Power Generator, **EC-PG**:
  For an integer $e \geq 2$, consider the sequence (with $Q_0 = P$),

  $$Q_k = eQ_{k-1} = e^k P, \qquad k = 1, 2, \ldots,$$

  Determining e from Q_k, Q_{k-1} would be solving the DLP.
  Constructing the following sequence element given longer substrings related to generalized Diffie-Hellman problem.

Elliptic curve PRNGs II

- EC Naor-Reingold Generator, **EC-NRG**:
  Given an integer vector $(a_1, \ldots, a_n)$, consider the sequence:

$$Q_{\mathbf{a},k} = a_1^{k_1} \ldots a_n^{k_n} P, \qquad k = 1, 2, \ldots,$$

  where $k = k_1 \ldots k_n$ is the bit representation of k,
  $0 \leq k \leq 2^n - 1$.

- **Example**:
  $n = 4$, $l = 19$ and $\mathbf{a} = (2, 5, 3, 4)$

$$f_{\mathbf{a},0} = 2^0 5^0 3^0 4^0 P = P, \qquad \ldots$$

$$f_{\mathbf{a},1} = 2^0 5^0 3^0 4^1 P = 4P, \qquad f_{\mathbf{a},11} = 2^1 5^0 3^1 4^1 P = 24P = 5P$$

$$f_{\mathbf{a},2} = 2^0 5^0 3^1 4^0 P = 3P, \qquad f_{\mathbf{a},15} = 2^1 5^1 3^1 4^1 P = 120P = 6P$$

$$f_{\mathbf{a},3} = 2^0 5^0 3^1 4^1 P = 12P$$

Character sums on elliptic curves

David Kohel, Igor Shparlinski, 2000:

Let $E/\mathbb{F}_p$ be an elliptic curve and $P \in H \subseteq E(\mathbb{F}_p)$ for some subgroup H. Then for any function f nonconstant on E we have

$$\sum_{P \in H} \exp\left(2\pi i \frac{f(P)}{p}\right) = O(p^{1/2})$$

Results

Florian Hess, T. L., Igor Shparlinski, 2002–2003:

> If the order ℓ of P is at least $p^{1/2+\varepsilon}$ then all above sequences (**EC-LCG**, **EC-PG**, **EC-NRG**) are reasonable well distributed.

EC power generator

$E/\mathbb{F}_q$ nonsupersingular, $q = p^r$, $T = \mathrm{ord}_\ell(e)$.

For any integer $\nu \geq 1$, the bound

$$\Delta_e(S^{\mathrm{PG}}) \ll T^{1-(3\nu+2)/2\nu(\nu+2)} \ell^{(\nu+1)/\nu(\nu+2)} q^{1/4(\nu+2)} (\ln p + 1)^r$$

holds for the discrepancy of the sequence S^{PG} obtained from the power generator.

(paper to appear, contains also linear complexity estimate)

Koblitz curves over $\mathbb{F}_2$

Koblitz curves are subfield curves

$$E_a : Y^2 + XY = X^3 + aX^2 + 1, \qquad a = 0, 1.$$

Consider curve over extension field $\mathbb{F}_{2^n}$.

Frobenius automorphism σ of field extension extends to points: $\sigma((x, y)) = (x^2, y^2)$

$$P \in E(\mathbb{F}_{2^n}) \Rightarrow \sigma(P) \in E(\mathbb{F}_{2^n})$$

If $\ell > (\#E_a(\mathbb{F}_{2^n}))^{1/2}$ then $\sigma^j(P) \in \langle P \rangle$. Assume this case in the sequel.

Scalar multiplication

Neal Koblitz, Jerome Solinas 1992–1999:
Every integer m allows unique NAF (non-adjacent form) such that

$$mP = \sum \mu_i \sigma^i(P), \;\; \mu_i \in \{0, \pm 1\}, \mu_i \mu_{i-1} = 0.$$

Hence, obvious use in above method – just use expansion of e.
In cryptographic protocols often computation of mP for random m is required.
Faster:

choose random NAF $(\mu_0, \mu_1, \ldots, \mu_{k-1})$, $\mu_i \in \{0, \pm 1\}$, $\mu_i \mu_{i-1} = 0$

to save time to compute expansion.

General results on NAF

Bosma, 2001:

$\mathcal{M}_k = \{(\mu_0, \ldots, \mu_{k-1}) \in \{0, \pm 1\}^k \mid \mu_j \mu_{j+1} = 0\}$

$$\#\mathcal{M}_k = \frac{4}{3} 2^k + O(1).$$

Distribution properties

For $k \leq n$ we consider the points

$$P_{\mathbf{m}} = \sum_{j=0}^{k-1} \mu_j \sigma^j(P), \qquad \mathbf{m} = (\mu_0, \ldots, \mu_{k-1}) \in \mathcal{M}_k.$$

Let $N_k(Q) = \#\{\mathbf{m} \in \mathcal{M}_{\mathbf{k}} \mid \mathbf{P_m} = \mathbf{Q}\}$.
For good distribution expect $N_k(Q) \sim \#\mathcal{M}_k/\ell$.

T. L., Igor Shparlinski, 2003:

$$N_k(Q) = O\left(\#\mathcal{M}_k/\ell\right)$$

Proof I

Let $1 \leq r \leq k$ and $2^r \leq \ell/8$.
Assume that $N_k(Q) \geq \#\mathcal{M}_{k-r} + 1$ solutions.
Then there are two distinct vectors

$$\mathbf{m}_\nu = (\mu_{\nu,\mathbf{0}}, \ldots, \mu_{\nu,\mathbf{k-1}}) \in \mathcal{M}_\mathbf{k}, \qquad \nu = \mathbf{1}, \mathbf{2},$$

with $P_{\mathbf{m_1}} = P_{\mathbf{m_2}} = Q$ and such that $\mathbf{m_1}$ and $\mathbf{m_2}$ agree at the last $k - r$ components.
Therefore,

$$\mathcal{O} = P_{\mathbf{m_1}} - P_{\mathbf{m_2}} = \sum_{i=0}^{r-1} d_i \sigma^i(P),$$

where $d_i = m_{1,i} - m_{2,i}$ and thus $|d_i| \leq 2$, $i = 0, \ldots, r-1$.

Proof II

The characteristic polynomial of E_a (and of σ) is

$$\chi_a(T) = T^2 + (-1)^a T + 2.$$

Assume that $\chi_a(T)$ is irreducible (the other case is similar ... but not too interesting).
Hence $\chi_a(T)$ and

$$F(T) = \sum_{i=0}^{r-1} d_i T^i$$

have a common root in the algebraic closure of $\mathbb{F}_\ell$.
Therefore,

$$\mathrm{Res}(\chi_a, F) \equiv 0 \pmod{\ell}.$$

Proof III

Let τ_1 and τ_2 be the roots of χ_a. Then

$$\mathrm{Res}(\chi_a, F) = F(\tau_1)F(\tau_2)$$

and $|\tau_1| = |\tau_2| = \sqrt{2}$.
Bounding $|F(\tau_j)|$, we get

$$|\mathrm{Res}(\chi_a, F)| < 2^{r+3} \leq \ell.$$

Hence, $\mathrm{Res}(\chi_a, F) = 0$. – Easy to rule out by looking at the constant coefficient of χ_a.

The End!