Monday, Jun 19th

Elliptic curve cryptography.

Diffie Hellman's protocol: Alice and Bob want to agree on a secret key:

Choose q, prime large enough, $\mathbb{F}_q^* = \langle g \rangle$ $g \equiv$ primitive root.

Public key: $\{q, g\}$.

Alice:
- choose $a \in \mathbb{Z}$
- sends $\xrightarrow{g^a \bmod q}$
- $\xleftarrow{g^b \bmod q}$
- compute $(g^b)^a = g^{ab} \bmod q$

Bob
- choose b
- sends
- compute $(g^a)^b = g^{ab} \bmod q$

An eavesdropper (Eve) sees g^a, g^b and to recover a, b (to get g^{ab}) must solve DLP:

input y

output $x \mid g^x = y \bmod q$, $\langle g \rangle = \mathbb{F}_q^*$.

Brute force: try $x \in \{1, .., q-2\}$, $O(q) = O(e^{s(q)})$ $s(q) = \log(q) \equiv$ size of q.

- **shanks algorithm (Baby step-giant step)**

$G = \langle \alpha \rangle$ cyclic group, order n. Given $\beta \in G$, want $x \in \mathbb{Z} \mid \alpha^x = \beta$.

We rewrite: $x = im + j$ $m = \lceil \sqrt{n} \rceil$, $0 \le i < m$, $0 \le j < m$

$\alpha^x = \beta \Leftrightarrow \alpha^{im+j} = \beta \Leftrightarrow \alpha^j = \beta(\alpha^{-m})^i$

- Precompute α^j, store (j, α^j) for $j \in \{0, .., m-1\}$;
- Compute α^{-m};
- $\gamma := \beta$
- for $i \in \{0, .. m-1\}$
  - check if γ is the second component of some pair $\to \alpha^j$
    - if so, $im + j$
    - if not, $\gamma := \gamma \cdot \alpha^{-m}$

Complexity of Shank's algorithm: $O(\sqrt{n})$ (number of multiplications in $\mathbb{F}_q$).

- <u>Can we perform an efficient multiplication (exponentiation)?</u>

$$x^n = \begin{cases} x\cdot(x^2)^{\frac{n-1}{2}} & \text{if } n \text{ is odd} \\ (x^2)^{\frac{n}{2}} & \text{if } n \text{ is even} \end{cases}$$

$n = \sum_{i=0}^{N} a_i 2^i \qquad a_i \in \mathbb{F}_2 \Rightarrow$ ~~want~~ $x^n = x^{\sum a_i 2^i}$

~~$m := 1$~~
~~$u := 1$~~
~~for $i = 0, \dots, N$~~
~~$u := 2u$~~
~~if $a_i = 1$~~
~~$m := m * x$;~~
~~$u := 2 * u$;~~

```
if n = 0 then return 1;
y := 1;
while n > 1 do
        if n odd then
              y := x * y;
        x := x * x;
        n := floor(n/2);
return y * x;
```

<u>Complexity</u>: at most $\lfloor \log_2 n \rfloor$ multiplications and $\lfloor \log_2 n \rfloor$ squarings.

- Number field sieve attack (factoring): $O\left(e^{(7\log(n))^{1/3}\cdot \log\log(n)}\right)$

- Shor's attack $O(\log(n)^3)$!!

- Elliptic curve discrete logarithm problem (ECDLP):

$E/\mathbb{F}_p$ elliptic curve, $Q \in E(\mathbb{F}_p)$ of large enough order $\leq p+1+2\sqrt{p}$.

given $P = nQ$, determine n.

We can use it for ECDH (elliptic curve Diffie-Hellman).

Choose $Q \in E(\mathbb{F}_p)$ of large enough order n.

Alice:

- Chooses $d_A \in \{1, \dots, n-1\}$
- Computes $Q_A = d_A Q$ $\xrightarrow{\text{sends}}$ Q_A
- computes $d_A(Q_B)$ $\xleftarrow{\text{sends}}$ Q_B

$\quad \parallel$

$d_A d_B Q$

Bob

- Chooses $d_B \in \{1 \dots n-1\}$
- computes $Q_B = d_B Q$
- Computes $d_B Q_A = d_B d_A Q$

Other ECDLP-based protocols:

- ECIES (elliptic curve integrated encryption scheme)
- ECDSA (elliptic curve digital signature algorithm).

- ECC was suggested by Koblitz and Miller (1985). ECC algorithm entered wide use in 2004-2005.

- NIST (1999). Recommends fifteen elliptic curves. ~~One of them~~,

FIPS-186-4 ten recommended finite fields:

- $\mathbb{F}_p$ $s(p) = 192, 224, 256, 384, 521$ bits
- $\mathbb{F}_{2^m}$ $m = 163, 233, 283, 409, 571$.

$\Big\}$ one elliptic curve for each field.

- Benefits over RSA/DH: smaller key sizes, 256-bit elliptic curve key provides comparable security to a 3072-bit RSA public key. The size of the EC determines the difficulty of DLP.

2. Smart's attack (if $|E(\mathbb{F}_p)| = p$.) $\rightsquigarrow n=1, k=p$.

$|E(\mathbb{F}_p)| = p \Rightarrow \quad a_p := ||E(\mathbb{F}_p)| - p - 1| = 1 = tr(\varphi_p)$

Let $E/\mathbb{F}_p$, consider $E(\mathbb{Q}_p): y^2 = x^3 + ax + b$ $\quad p \nmid \Delta$.

$$\downarrow \text{Red}$$

$$E(\mathbb{F}_p): y^2 = x^3 + \bar{a}x + \bar{b}.$$

$\Rightarrow$ Red : $E(\mathbb{Q}_p) \longrightarrow E(\mathbb{F}_p)$ homomorphism.

$(x,y) \longmapsto (\bar{x}, \bar{y})$

$E_1(\mathbb{Q}_p) = \mathrm{Ker}(\text{Red})$, rather, can think as those points which reduce to ∞, if we take it to be $(0:0:1)$.

· p-adic elliptic logarithm: $\psi_p : E_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ (Sil VII).

$S \in E_1(\mathbb{Q}_p)$, $\psi_p(S) := -\dfrac{x(S)}{y(S)}$.

Attack: $Q = kP$; $Q, P \in E(\mathbb{F}_p)$, $|E(\mathbb{F}_p)| = p$.

lift P, Q to $E(\mathbb{Q}_p)$ by Hensel's lemma $\rightsquigarrow P', Q'$.

$Q = kP \Rightarrow Q' - kP' \in E_1(\mathbb{Q}_p)$.

Now $E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong E(\mathbb{F}_p)$, ord $p \Rightarrow pE(\mathbb{Q}_p) \subseteq E_1(\mathbb{Q}_p)$.

$\Rightarrow pQ' - kpP' \in E_1(\mathbb{Q}_p)$.

$\psi_p(pQ') - k\psi_p(pP') \in p\mathbb{Z}$ $\Rightarrow k = \dfrac{\psi_p(pQ')}{\psi_p(pP')} \mod p$.

e.g. $y^2 = x^3 - 3x + b \ / \mathbb{F}_p$

P-192, $p = 2^{192} - 2^{64} - 1$

standard curve database

Secp192r1 prime192v1

Notice: $E(\mathbb{F}_q) \cong C_n \oplus C_{nk}$.

$E(\mathbb{F}_q) \cong C_{n_1} \oplus \ldots \oplus C_{n_r}$ $\quad n_i | n_{i+1}$

$\Rightarrow E(\mathbb{F}_q)$ has n_1^r points of order $| n_1$

$|E[n_1]| \leq n_1^2 \Rightarrow r \leq 2$ #

• weak curves

• 1. Pohlig-Hellman attack:

reduces ECDLP in $E(\mathbb{F}_p)$ to ECDLP in prime subgroups of $\langle P \rangle$, the subgroup generated by P.

$n = |\langle P \rangle|$ $\quad n = p_1^{e_1} \ldots p_r^{e_r}$ $\quad Q, P \in E(\mathbb{F}_p)$, $Q = kP$ $\quad k$?

we will compute $k_i \equiv k \mod p^{e_i}$ and by CRT $\leadsto k$.

$k_i = z_0 + z_1 p_i + \ldots + z_{e-1} p_i^{e_i - 1}$. Compute k_i:

$P_0 := \frac{n}{p_i} P$, $Q_0 := \frac{n}{p_i} Q \Rightarrow p_i P_0 = P \Rightarrow$

$Q_0 = \frac{n}{p_i} Q = \frac{n}{p_i} kP = k \frac{n}{p_i} P = k P_0 = k_i P_0$

$\uparrow k = k_i \mod p_i^{e_i}$.

Since the ord of P_0 is p_i and z_0 is the 1st digit of base p integer

$\Rightarrow kP_0 = z_0 P_0$ $\Rightarrow$ solve $Q_0 = z_0 P_0$, $z_0 \in \{0, 1, \ldots, p_i - 1\}$.

$\quad \overset{\shortparallel}{k_i P_0}$

iterating (Han04) we get z_j by solving $Q_j = z_j P_0$ s.t.

$$Q_j = \frac{n}{p_i^{j+1}} (Q - z_0 P - z_1 p_i P - z_2 p_i^2 P - \ldots - z_{j-1} p_i^{j-1} P)$$

Han04: Hankerson, Vanstone, Menezes: Guide to elliptic curve cryptography.

Menezes - Okamoto - Vanstone attack (MOV)

L prime $\langle P \rangle \subseteq E(\mathbb{F}_p)$ order L.

~~α: ...~~ $\alpha : L \hookrightarrow \mathbb{F}_{p^k}^*$ $\quad \mathbb{F}_{p^k} | \mathbb{F}_p$ extension of degree k.

solve DLP in $\mathbb{F}_{p^k}$ with order $O(e((7\log(p^k))^{1/3}))$.

Necessary and sufficient conditions for MOV to be carried out:

$L | p^k - 1$, $\exists L^2$ points of order 1 or L in $E(\mathbb{F}_{p^k})$.

<u>Thm</u>: If $E/\mathbb{F}_q$ is supersingular, then the reduction of the ECDLP to the DLP in $\mathbb{F}_{q^k}$ is a probabilistic poly time (in $s(q) = \ln q$) reduction

<u>Cor</u>: $P \in E(\mathbb{F}_q)$, E supersingular, P of order n.
Let $R = \ell P \in E(\mathbb{F}_q)$. MOV determines ℓ in probabilistic ~~poly~~ <u>subexp.</u> time

<u>Key</u>: the Weil pairing (in Sil III).

$e_n : E[n](\bar{\mathbb{F}}_q) \times E[n](\bar{\mathbb{F}}_q) \longrightarrow \mu_n(\bar{\mathbb{F}}_q)$, s.t.:

i) $e_n(P,P) = 1$
ii) $e_n(P_1,P_2) = e_n(P_2,P_1)^{-1}$
iii) $e_n(P_1+P_2,P_3) = e_n(P_1,P_3) \cdot e_n(P_2,P_3)$ same in the right slot.
iv) $P_1 \in E[n]$. If $e_n(P_1,P) = 1 \;\forall P \in E[n] \Rightarrow P_1 = O$. Same in the right slot.
v) $E[n] \subseteq E(\mathbb{F}_{q^k}) \Rightarrow e_n(P_1,P_2) \in \mathbb{F}_{q^k} \;\forall P_1,P_2 \in E[n]$.

<u>Alg</u>: input $P \in E(\mathbb{F}_q)$, order n_1, $R = \ell P$. $\quad$ ($E(\mathbb{F}_q) = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$) $n_2 | n_1$.
output: $\ell' \equiv \ell \mod n'$, $n' | n_2$.

i) Pick $T \in E(\mathbb{F}_q)$ at random
ii) Compute $\alpha = e_{n_1}(P,T)$, $\beta = e_{n_1}(R,T) = e_{n_1}(P,T)^\ell = \alpha^\ell$
iii) Compute ℓ', DLP of $\beta = \alpha^\ell$ in $\mathbb{F}_q$.

M,O,V: Reducing elliptic curve logarithms to logarithms in a finite field.

Tuesday, 20

Elliptic curves over $\mathbb{Q}$

Thm: $E/\mathbb{Q}$ elliptic curve $\Rightarrow$ $E(\mathbb{Q})$ is finitely generated.

The proof consists in several steps (Sil-Ta Ch. III).

• heights:

$x = \frac{m}{n} \in \mathbb{Q}$ in lowest terms, define $H(x) := \max\{|m|, |n|\} \in \mathbb{N}$. It's a good tool to measure "how complicated" a rational number is. For instance,

$h(x) := \log H(x)$.

$r = \frac{99999}{1000000} \approx 1$, $H(r) = 1000000$.

Lem: $\forall M$, $\{r \in \mathbb{Q} \mid H(r) \leq M\}$ is finite.

Proof: Indeed, finitely many posibilities ($\lceil M \rceil$) for numerator and denominator.

Def: Let $E: y^2 = x^3 + ax^2 + bx + c$ be a rational elliptic curve.

$P = (x, y) \in E(\mathbb{Q})$, define $H(P) = H(x)$, $h(P) = h(x)$.

$H(O) := 1$.

Lemma 1 in Sil-Ta.

Prop: $\{P \in E(\mathbb{Q}) \mid H(P) \leq M\}$ finite for each $M \in \mathbb{R}$.

Proof: Finitely many choices for the x-coordinate, and for each x, at most 2 possibilities for y.

Lemma 2: Let $P_0 \in E(\mathbb{Q})$. There is $K_0 = K(P, a, b)$ s.t.

$h(P + P_0) \leq 2h(P) + K_0$. (Home)

Lemma 3: $\exists K = K(a, b, c)$ s.t. $h(2P) \geq 4h(P) - K$ $\forall P \in E(\mathbb{Q})$.

Lemma 4: (The key!!) $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ finite.

Assuming these lemmas, we can conclude Mordell's thm by using:

Descent theorem

Let Γ be a commutative group. Suppose $h: \Gamma \to [0, \infty)$ s.t

a) $\forall M \in \mathbb{R}$, $\{P \in \Gamma \mid h(P) \leq M\}$ finite.

b) $\forall P_0 \in \Gamma$, $\exists K_0 = K(P_0, P)$ s.t. $h(P+P_0) \leq 2h(P) + K_0$ $\forall P \in \Gamma$.

c) $\exists K$ s.t $h(2P) \geq 4h(P) - K$ $\forall P \in \Gamma$.

d) $[\Gamma : 2\Gamma]$ finite

$\Rightarrow \Gamma$ is f.g.

Proof: Let $\{Q_1, Q_2, \dots, Q_n\}$ be representatives for the cosets of $\Gamma / 2\Gamma$.

$\forall P \in \Gamma$, $P - Q_{i_1} \in 2\Gamma \Rightarrow$

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m. \end{aligned}$$

idea: if $P_i \simeq 2P_{i+1} \Rightarrow h(P_{i+1}) \simeq \frac{1}{4} h(P_i) \Rightarrow \{P, P_1, \dots\}$ should have a decreasing height and we end up in a set of points with bounded height $\Rightarrow$ finite.

$$P = Q_{i_1} + 2P_1 = Q_{i_1} + 2Q_{i_2} + 4P_2 = Q_{i_1} + 2Q_{i_3} + 4Q_{i_3} + \dots + 2^{m-1} Q_{i_m} + 2^m P_m.$$

by b) $h(P-Q_i) \leq 2h(P)+K_i \qquad K_i \sim K(Q_i)$.

$\Rightarrow h(P-Q_i) \leq 2h(P)+K'$, $K' = \max\{K_i\}$.

by c) $4h(P_j) \leq h(2P_j)+K = h(P_{j-1}-Q_{i_j})+K \leq 2h(P_{j-1})+K'+K$

$\Rightarrow h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{K'+K}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1})-(K'+K)\right)$.

hence, if $h(P_{j-1}) \geq K'+K \Rightarrow h(P_j) \leq \frac{3}{4}h(P_{j-1})$.

$\Rightarrow$ In $\{P, P_1, P_2, \dots, P_m, \dots\}$ as long as P_j satisfies $h(P_j) \geq K'+K$ the next point will have $h(P_{j+1}) \leq \frac{3}{4}P(h_j) \Rightarrow h(P_m) \leq K'+K$

$\Rightarrow P = aQ_1 + aQ_2 + \dots + a_nQ_n + 2^m R \quad | \ h(R) \leq K'+K$ #.

finitely many, by lemma 1

Def (The Néron-Tate canonical height). $P \in E(\mathbb{Q})$

$$\hat{h}(P) = \frac{1}{2}\lim_{n\to\infty} \frac{h(2^nP)}{4^n}$$

Thm: $E/\mathbb{Q}$ elliptic curve, $\hat{h}$ canonical height. Then

a) $\forall P, Q \in E(\mathbb{Q})$, $\hat{h}(P+Q)+\hat{h}(P-Q) = 2\hat{h}(P)+2\hat{h}(Q)$

b) $\forall m \in \mathbb{Z}$, $P \in E(\mathbb{Q})$, $\hat{h}(mP) = m^2\hat{h}(P)$

Cor: $\langle \cdot,\cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$

$(P,Q) \mapsto \langle P,Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$

is bilinear (Néron-Tate pairing).

Notice: $P \in E[n](\mathbb{Q}) \Rightarrow \hat{h}(nP) = n^2\hat{h}(P) \Rightarrow \hat{h}(P) = 0$

$\hat{h}(nP) = \hat{h}(O) = 0$

Moreover, if $\hat{h}(P) = 0 \Rightarrow P$ torsion (requires proof!!)

Hence, we have proved:

<u>Thm</u> (Mordell): $E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$ $\quad r = \operatorname{rank}(E(\mathbb{Q}))$.

Barghava (2014): About 60% of elliptic curves have $r \leq 1$.

The Birch and Swinnerton-Dyer's conjecture

<u>version 1</u> (1963)

$$\prod_{p \text{ prime} \leq x} \frac{N_p}{p} \sim \log(x)^r \quad \text{for } x >> 1. \qquad (N_p = |E(\mathbb{F}_p)|)$$

If this is true and $r \geq 1$ one expects $N_p > p$ for p large enough

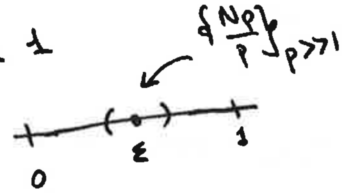
$\Rightarrow$ Smart's attack doesn't apply.

Notice that $\prod_{p \text{ prime} \leq x} N_p/p$ converges $\Rightarrow$ $\frac{N_p}{p} \to 1$

if $\frac{N_p}{p} \to \varepsilon < 1$

$\Downarrow$

$\prod_{p \leq x} \frac{N_p}{p} \to 0.$



Hence, if BSD is true $\Rightarrow$

$\frac{N_p}{p} > 1$ in the large.

<u>Version 2</u> (1967, I think...)

<u>Recall</u>: if $p \nmid \Delta$ we say that E has good reduction at p.

if ~~p~~ $p \mid \Delta$ we say that E has bad reduction at p.

<u>Def</u>: Suppose E has bad reduction at p.

a) if $E/\mathbb{F}_p$ has a cusp (i.e 1 tangent at the singular point) we say "E has additive bad reduction at p". Otherwise (2 tangents, node)

~~b)~~ we say that "E has multiplicative reduction at p".

<u>Prop</u>: E multiplicative red $\Leftrightarrow$ $p^2 \nmid \Delta$.

If $E: y^2 = x^3 + ax^2$ has multiplicative reduction at p then:

$E/\mathbb{F}_p$: $y^2 - ax^2 + x^3 = 0$, $(y + \sqrt{a}x)(y - \sqrt{a}x) + x^3 = 0$

$\sqrt{a} \in \mathbb{F}_{p^2}$.

<u>Def</u>: If $\sqrt{a} \in \mathbb{F}_p$ we say that E has "split multiplicative reduction at p" otherwise "non-split multiplicative reduction".

<u>Def</u>: The Hasse-Weil zeta function of $E/\mathbb{Q}$:

p prime $L_p(E,s) = \begin{cases} 1 - a_p p^{-s} + p^{1-2s} & p \nmid \Delta \\ 1 - a_p p^{-s} & p \mid \Delta,\ p^2 \nmid \Delta \\ 1 & p^2 \mid \Delta \end{cases}$

where, if $p^2 \nmid \Delta$: $a_p = \begin{cases} 1 & \text{split reduction} \\ -1 & \text{non-split.} \end{cases}$

$$L(E,s) := \prod_{p \text{ prime}} L_p(E,s)^{-1}$$

<u>obs</u>: Notice that for $p \nmid \Delta$, $L_p(E,s)$ is the numerator of the local zeta function for $E/\mathbb{F}_p$. ("L polynomial").

<u>Conj BSD version 2</u>: $\operatorname{ord}_{s=1} L(E,s) = r$.

<u>But</u>: $L(E,s)$ is only defined for $Re(s) > 3/2$. ($\leftarrow$ Hasse bound, home).

Relation between vs 1 and vs 2? Euler-like argument:

$$L(E,1) = \prod_p \frac{1}{1 - a_p p^{-1} + p^{-1}} = \prod_p \frac{p}{p - a_p + 1} = \prod_p \frac{p}{N_p}$$

suppose defined!!

If $rk = 1 \Rightarrow L(E,x) \simeq \frac{1}{\log(x)^r}$ $x \ll 1$.

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad$ "$x^r + \dots$"

Known results,

① Coates–Wiles: If $rk = 0 \Rightarrow L(E,s) \neq 0$.

Rather, how to make $L(E,s)$ defined near $s=1$?

Wiles modularity theorem (Taylor, Wiles, ...)

Def: A modular form (cusp) of weight k for $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \right\}$, $N | c$

if $f : \mathcal{H} \longrightarrow \mathbb{C}$ holomorphic s.t $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z). \quad + \text{"mild conditions" at } \infty. \quad (\text{want } f(z) \to 0 \text{ as } z \to r \in \mathbb{Q}.)$$

Since $f(z+1) = f(z) \Rightarrow f(z) = \sum_{n=1}^{\infty} a_n q^n \quad q = e^{2\pi i z}$

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad Re(s) \geq \frac{k}{2}.$$

Def: $E/\mathbb{Q}$ is modular if $\exists f \in S_2(\Gamma_0(N))$ s.t. $N = rad(\Delta)$ (essentially).

$$L(E,s) = L(f,s)$$

Thm (Taylor–Wiles, Annals 1995). Let $E/\mathbb{Q}$ be an elliptic curve

$\Rightarrow$ there exists $f \in S_2(\Gamma_0(N))^{new}$ s.t $L(E,s) = L(f,s)$.

For $f \in S_2(\Gamma_0(N))^{new}$ $L(f,s)$ extends to a holomorphic function in $\mathbb{C}$.

Hence, Coates–Wiles makes sense!! (and BSD!!)

Thm (Gross–Zagier) $E/\mathbb{Q}$ (modular) $\Rightarrow$ It is $L'(E,1) = \hat{h}(P).k$

P non torsion, $P \in E(\mathbb{Q}(\sqrt{D}))$ "Heegner point" and $k \neq 0$.

hence, if $L'(E,1) \neq 0 \Rightarrow rk(E(\mathbb{Q})) \geq 1$

Thm (Kolyvagin). ~~If $rk(E(\mathbb{Q})) = 1 \Rightarrow ord_{s=1}(L(E,s)) \geq 1$~~.

Conditions as before, $rk(E(\mathbb{Q}(\sqrt{D}))) = 1$

$\Longrightarrow rk(E(\mathbb{Q})) \leq 1$.