Elliptic-curve factoring, witnesses and oracles

Jacek Pomykała

UW
MIM
Wydział
Matematyki, Informatyki i Mechaniki

Military University of Technology and University of Warsaw

NuTMiC 2024

Szczecin, 25 June 2024

Schedule of presentation

- Preliminaries on elliptic curves over $\mathbb{Z}_N$ and partially smooth numbers
- Separating witnesses and separating sets
- Multiplicative functions approach
- Oracle factorization and rigorous approach

Schedule of presentation

- **Preliminaries on elliptic curves over $\mathbb{Z}_N$ and partially smooth numbers**
- Separating witnesses and separating sets
- Multiplicative functions approach
- Oracle factorization and rigorous approach

Preliminaries on $E(\mathbb{Z}_N)$, part 1

- Let $N = \prod_{i=1}^{s} p_i$ be a squrefree number coprime to 6.
- The projective plane $\mathbb{P}^2(\mathbb{Z}_N)$ is defined to be the set of equivalence classes of primitive triples in $\mathbb{Z}_N^3$ (i.e., triples (x_1, x_2, x_3) with $\gcd(x_1, x_2, x_3, N) = 1$) with respect to the equivalence:

$$(x_1, x_2, x_3) \sim (y_1, y_2, y_3) \text{ iff } (x_1, x_2, x_3) = u(y_1, y_2, y_3)$$

for a unit $u \in \mathbb{Z}_N^*$.

Preliminaries on $E(\mathbb{Z}_N)$, part 2

- An **elliptic curve** over $\mathbb{Z}_N$ is given by the short Weierstrass equation $E : y^2z = x^3 + b_1xz^2 + b_2z^3$, where $b_1, b_2 \in \mathbb{Z}_N$ and the discriminant $-16(4b_1^3 + 27b_2^2) \in \mathbb{Z}_N^*$.
- The point $O = (0 : 1 : 0)$, called the zero point, belongs to $E(\mathbb{Z}_N)$.
- Let $V(E(\mathbb{Z}_N)) = \{(x, y) \in E(\mathbb{Z}_N)\} \cup \{O\}$ be the set of finite points in $E(\mathbb{Z}_N)$ along with O.
- For each equivalence class (point) $(x : y : z) \in E(\mathbb{Z}_N) \setminus V(E(\mathbb{Z}_N))$ the $\gcd(z, N)$ is a nontrivial divisor of N.

Preliminaries on $E(\mathbb{Z}_N)$, part 3

- Let $E(\mathbb{Z}_{p_i})$ be the group of $\mathbb{Z}_{p_i}$-rational points on the reduction E mod p_i for primes $p_i \mid N$.
- If $E(\mathbb{Z}_N)$ is the set of points in $\mathbb{P}^2(\mathbb{Z}_N)$ satisfying the equation of E then by CRT there exists the bijection

$$\varphi : E(\mathbb{Z}_N) \to \prod_{i=1}^{s} E(\mathbb{Z}_{p_i}) \tag{1}$$

  induced by the reductions mod p_i.
- The points $(x : y : z) \in E(\mathbb{Z}_N)$, with $z \in \mathbb{Z}_{\mathbb{N}}^*$, **can be written as** $(x/z : y/z : 1)$ and are called finite points.
- The set $E(\mathbb{Z}_N)$ is an additive group for which φ is a group isomorphism, which in general can be defined using the so-called complete set of addition laws on E.

Preliminaries on $E(\mathbb{Z}_N)$, part 4

In order to **add two finite points** $\bar{P}, \bar{Q} \in E(\mathbb{Z}_N)$ we can also **use the same formulas** as for elliptic curves over fields in the following case: for $\varphi(\bar{P}) = (P_1, \ldots, P_s)$ and $\varphi(\bar{Q}) = (Q_1, \ldots, Q_s) \in \prod_{i=1}^{s} E(\mathbb{Z}_{p_i})$ if either $Q_i \neq \pm P_i$ or $Q_i = P_i$ and $Q_i \neq -P_i$, for each i.
Then

$$x_{\bar{P}+\bar{Q}} = \lambda^2 - x_{\bar{P}} - x_{\bar{Q}} \tag{2}$$

$$y_{\bar{P}+\bar{Q}} = \lambda(x_{\bar{P}} - x_{\bar{P}+\bar{Q}}) - y_{\bar{P}}, \tag{3}$$

where

$$\lambda = \frac{y_{\bar{Q}} - y_{\bar{P}}}{x_{\bar{Q}} - x_{\bar{P}}}$$

if $Q_i \neq \pm P_i$ for each i, or $\lambda = \frac{3x_{\bar{P}}^2 + a}{2y_{\bar{P}}}$ if $Q_i = P_i$ and $Q_i \neq -P_i$ for each i.

Preliminaries on $E(\mathbb{Z}_N)$, part 5

- Let $\bar{P}, \bar{Q} \in E(\mathbb{Z}_N)$ **and if** $\bar{R} = \bar{P} + \bar{Q}$ is **finite** then the formula (1) **give** the **coordinates of the resulted point** $\bar{R}$.
  Otherwise, either we find a nontrivial divisor of N **or** prove that all local orders $ordR_i$ are **equal to each other** for $i = 1, 2, ..., s$.
- The the familiar ECF is based on the computation of points in E over $\mathbb{Z}_N$ **with** the **hope** of **obtaining** the **nontrivial divisor** of N provided some local order of point $\bar{P} \in E(\mathbb{Z}_N)$ is $Y-$smooth number for **subexponential size** of Y. In this connection we choose randomly x, y and b_1, while b_2 is **determined** by the **equation** of the **curve** over $\mathbb{Z}_N$.
- Throughout the presentation we let $\Delta_{\bar{b}} := 6(4b_1^3 + 27b_2^2)$ be **coprime** to N and $\bar{P} \in E(\mathbb{Z}_N)$, while in case when $s = 2$ then φ sends the point $\bar{P}$ to $\varphi(\bar{P}) := (P, P')$.

Preliminaries on $E(\mathbb{Z}_N)$, part 6

- Let $N = pq$, where $3 < p < q < \vartheta p$ for a fixed $\vartheta > 1$ and $Y = Y(N)$.
- The largest Y-smooth divisor of m is denoted by $s_Y(m)$.
- The computation of finite point mQ takes $O(\log m)$ adding operations in $E(Z_N)$. Hence for Y-smooth number $m = m_Y$ represented as $m_Y = p_k^{e_k} \dots 3^{e_3} 2^{e_2}$, where $e_i = e_i(N)$ is the highest exponent of p_i such that $p_i^{e_i}$ does not exceed $\min(p,q) + 2\sqrt{\min(p,q)} + 1$, the computation of $m_Y Q$ takes

$$\ll \log N \sum_{i \le k} \log(p_i) = O(B \log N) = B^{1+o(1)} \tag{4}$$

  additions in $E(Z_N)$ in view of the PNT, as $N \to \infty$.
- Looking more carefully $\Rightarrow$ that one can **decompose** $N = pq$ in time $Y^{2+o(1)}$, **provided** the local orders of point $\bar{P} \in E(Z_N)$, $ordP \neq ordP'$ differ on some power of prime $l \le Y$, which we **state alternatively as** $s_Y(ordP) \neq s_Y(ordP')$.

Classical compositness and factoring witnesses

- We consider first the classical case corresponding to the group $\mathbb{Z}_N^*$ and important from cryptological point of view case $N = pq$.
- The Fermat-Euclide (compositness) witness for N is $a \in \mathbb{Z}_N^*$ satisfying the condition

$$v_l(\mathrm{ord}_p a) \neq v_l(\mathrm{ord}_q a),$$

for some prime $l \mid ord_N a$, where $v_l(m)$ is the highest exponent of l dividing m.

Classical factoring witness, part 2

- The first challenge in general is to focus on small values $a \leq A = A(N)$, reducing the problem of factoring N to small values of Dirichlet character's non-residues or more generally small generating sets of $\mathbb{Z}_N^*$.
- The second one concerns small values of $l \leq B = B(N)$, related to well known Pollard's $p-1$ or Williams $p+1$ methods of factoring. Both A and B-aspects are important in the deterministic approach to factoring integers.
- We will exploit the second approach for the "shifted" primes of the form $r+1-a_E(r)$, where $r \in \{p,q\}$ and $a_E(r)$ is the Frobenius trace of E modulo r. In what follows we use the equality $\varphi(\bar{P}) = (P, P')$, for $\bar{P} \in E(\mathbb{Z}_N)$ refering to the the familiar Lenstra's ECF method for $N = pq$.

Partially **smooth numbers**: $(B,\beta,D)-$smooth and $(B,\beta,D,\sigma)-$smooth

The maximal $Y-$smooth factor of m is called shortly $Y-$factor of m. Moreover we call m $(B,\beta,D)-$smooth if it is $D-$smooth and

$$s_B(m) \geq m^{\beta}.$$

We call m $(B,\beta,D,\sigma)-$smooth, if (in principle) additionally we have that $(m/s_B(m))^* \leq D^{\sigma}$, where d^* denotes the maximal squarefree factor of d. We use the notation (I,B,β,D,σ) to underline that $m \in I$.

Partially smooth and **admissible** elliptic curves over $\mathbb{Z}_N$.

- By $B-$smooth, $(B,\beta,D)-$ or (B,β,D,σ)-smooth elliptic curve over $\mathbb{Z}_N$ we mean the curve E whose some local order is such number.
- Restricting yourselves to $Y-$smooth curves we state the more involved definition. Namely let $0 \leq \gamma \leq 1$ and $c = c(\vartheta)$ be fixed. We call $Y-$smooth elliptic curve E $(Y,\gamma)-$admissible if the following conditions hold

$$\gcd(E_p, E_q) \geq N^{1/2-\gamma/2} \tag{5}$$

and

$$1 \leq \min(a_E(p), a_E(q)) \leq c(\vartheta) N^{1/4-\gamma/2}. \tag{6}$$

The admissible elliptic curves play the significant role in investigating the separating witnesses for N and finding decomposition $N = pq$.

Schedule of presentation

- Preliminaries on elliptic curves over $\mathbb{Z}_N$ and partially smooth numbers
- **Separating witnesses and separating sets**
- Multiplicative functions approach
- Oracle factorization and rigorous approach

Polylog$N$ conditional factoring results

Theorem 1 (*Dieulefait, Jimenez Urroz* **2020**)

Given $N = pq$, arbtrarily small $\varepsilon > 0$ and elliptic curve $E(\mathbb{Z}_N)$ uniformly at random, there exists a polynomial time algorithm that with input N and the factorization of E_N outputs the factors p and q with probability $1 - \varepsilon$.

In fact having E_N with $\Omega(E_N) = O(\log\log N)$ the algorithm can be derandomized and runs in deterministic polylog(N) time by the Coppersmith result.

Polylog$N$ conditional elliptic Fermat approach - Part 1

The classical Fermat's factoring method allows to efficiently (in deterministic time polylog$N$) factor a positive integer N provided $N = n_1 n_2 = pq$, where the absolute value of $n_1 - n_2$ is of order of magnitude $N^{1/4}$, since then we are able to find the related divisor close to $\sqrt{n_1 n_2} = \sqrt{N}$.
Considering the linear forms of type $F^{\pm} := F^{\pm}(a, b) = ap \pm bq$, where the coefficients a, b are related to the given elliptic curves $E(\mathbb{Z}_p)$ and $E(\mathbb{Z}_q)$ respectively, one can deduce the conditional factoring results applying the extension of Fermat idea for the above linear forms with coefficients $a_r(E)$ or E_r, where $r \in \{p, q\}$.

Polylog(N) conditional factoring results - Part 2

Theorem 2 (*Pomykała, Żołnierczyk* **2024**)

Let $N = pq$, where p, q are sufficiently large, $q \in [Mp, 2Mp]$, where $M < N^{1/3}$ and E_N be given. Then we have

(i) *Let $A = \{a_p(E), a_q(E)\}$. Assume that for some $D = D(N) \geq 1/2$, some $a \in A$ and $b = A \setminus \{a\}$ we have*

$$\left| \frac{p}{q} - \frac{a}{b} \right| \leq \frac{1}{D} \tag{7}$$

Then we can factor N in deterministic time

$$t = t(M, D, a_p(E), a_q(E)) = (\log N)^{O(1)} \left(M \left(1 + \left(\frac{|a_p(E)| + |a_q(E)|}{D} \right)^2 \right. \right. \tag{8}$$

Theorem - cont. Part 3

(ii) Let $d \mid \gcd(E_p, E_q)$ be given.
Let N, E_N and $d \mid \gcd(E_p, E_q) > 1$ be given. Assume that for some α and $|\theta_1| \leq 1$, $s \neq d$, $s \mid d^2$, the following condition

$$\left(\frac{s}{d}\right)^2 = 1 + \frac{1}{D} + \left(\frac{\alpha\theta_1}{D^2}\right), \tag{9}$$

holds true and

$$\frac{p}{q} - \frac{E_p}{E_q} = \frac{p}{q}\left(\frac{1}{D} + \frac{\beta\theta_2}{D^2}\right) \tag{10}$$

for some $\beta = \beta(\alpha)$ and $|\theta_2| \leq 1$.
Then we can detect p, q in deterministic time $2^{\Omega(d)}\frac{NM^2}{D^4}(\log N)^{O(1)}$.
In particular letting $M = polylogN$ and $D = \Theta(N^{1/4})$ we compute the decomposition $N = pq$, in deterministic polynomial time, provided $2^{\Omega(d)} = (logN)^{O(1)}$.

Separating witnesses and separating sets, part 1

Definition 3

Let E be B-smooth elliptic curve. The point $\bar{P} \in E(\mathbb{Z}_N)$ is called (E, B)-separating witness if

$$s_B(\mathrm{ord} P) \neq s_B(\mathrm{ord} P'), \tag{11}$$

where $\varphi(\bar{P}) := (P, P')$.

Definition 4

Let E be (B, β, D)-smooth elliptic curve. The point $\bar{P}$ is called (E, B, D)-separating witness if it is $(E, D)-$separating witness but not $(E, B)-$separating witness for N.

Separating witnesses and separating sets, part 2

- Let Y be either B or D ($D > B$) and $I_r \in [r+1-\sqrt{r}, r+1+\sqrt{r}] \subseteq I = [r+1-2\sqrt{r}, r+1+2\sqrt{r}]$.
- The set **X** is called (E, Y)-separating set if it contains some $(E, Y)-$separating witness $\bar{P}$. It is $(E, B, D)-$separating set if it is (E, D)-separating but not (E, B)-separating set.

Polylog$N$ factoring result, part 1

Using only the equations $E_r = r + 1 - a_E(r)$ for $r \in \{p, q\}$ the knowledge of E_r for some r does not imply the decomposition $N = pq$ in polylog$N$ time.
However it is implied by the *Coppersmith method* (**1994**). Below we state the result on a weaker conditions sufficient to decompose $N = pq$ in polynomial time.
In this point we see the connection with the factoring N with the knowledge $E_N := E_p E_q$ and the oracle factorization discussed further.

Polylog$N$ factoring result, part 2

Theorem 5 (Pomykała, Żołnierczyk **2024)**

Let $\gamma \in [0, 1/4)$ *and* $N = pq \geq N_0$ *is sufficiently large, where* $p < q < \vartheta p$. *Assume that we know the value* d *such that*

(i) $d := \gcd(s_B(E_p)s_B(E_q)) \geq N^{\frac{1}{2}-\frac{\gamma}{2}}$
or

(ii) $d = s_B(\mathrm{ord}R) = s_B(\mathrm{ord}R') \geq N^{\frac{1}{2}-\frac{\gamma}{2}}$ *for some* $\gamma \in [0, 1/4)$,

where

$$1 \leq \min(a_E(p), a_E(q)) \leq c(\vartheta)N^{\frac{1}{4}-\frac{\gamma}{2}} \tag{12}$$

for some $c(\vartheta) > 0$ *and* $\bar{R} \in E(\mathbb{Z}_N)$. *Then the decomposition* $N = pq$ *can be discovered in deterministic plynomial time polylog*N.
The same conclusion holds *provided* $r/s_B(E_r) = (\log N)^{O(1)}$ *for some* $r \in \{p, q\}$.

Polylog$N$ factoring result - Main idea, part 1

- The main step of the proof is the following. By the familiar (mentioned above) arguments we can **exceed this complexity bound to polynomial time**, provided either the greatest common divisor of B-factors of E_r and $E_{r'}$ is large (and known), or the B-factors of local orders $\mathrm{ord}P$ and $\mathrm{ord}P'$ of the point $\bar{P} \in E(\mathbb{Z}_N)$ are the same and large (which in fact implies the $(B,\gamma)-$admissibility of E).
- Now let $d = \gcd(E_p, E_q)$. Then $E_p = dr_p$, $E_q = dE_q$ and representing N in base d we have

$$N = c_0 + c_1 d + c_2 d^2. \tag{13}$$

Polylog$N$ factoring result - Main idea, part 2

Letting $t_r = a_E(r) - 1$ for $r \in \{p, q\}$, we obtain

$$\begin{aligned} N = pq &= (dr_p + a_E(p) - 1)(dr_q + a_E(q) - 1) \\ &= (dr_p + t_p)(dr_q + t_q) = r_p r_q d^2 + (r_p t_q + r_q t_p)d + t_p t_q \end{aligned}$$

where $t_p, t_q \geq 0$.
Thus the coefficients r_p, r_q, t_p, t_q are uniquely defined by c_i ($i = 1, 2$) provided all they are in the interval $[0, d)$ and one can compute them in polylog$N$ time solving the relates system of equations.

Separating sets and (E, B)-factoring

- We recall that $\mathbf{X}$ is called **separating** set for N if it contains a separating witness for N.
- By $G_{\mathbf{X}}$ we mean the subgroup of $E(\mathbb{Z}_N)$ generated by the set $\mathbf{X}$ and $G_{B,\mathbf{X}}$ being the homomorphic image of $\mathbf{X}$ under the homomorphism Φ_N^B sending the point (P, P'), to (Q, Q'), where $Q = \frac{E_p}{s_B(E_p)} P$ and $Q' = \frac{E_q}{s_B(E_q)} P'$.
- Let $\boldsymbol{X} \subseteq E(\mathbb{Z}_N)$ be nonempty. Below we state and prove the results on the sufficient condition for the set $\mathbf{X}$ to contain some (E, B)-separating witness and, as a consequence the decomposition $N = pq$ in deterministic time $|\mathbf{X}| B^{2+o(1)}$, as N tends to infinity.

Result on (E, B)-factoring

The following theorem shows the sufficient condition for E over $\mathbb{Z}_N$ guaranteeing the existence of the separating witness in the set $\bar{X}$.

Theorem 6 (Jurkiewicz, Pomykała, Prabucka, Żołnierczyk **2024**)

Let $N = pq$, where $p < q < \vartheta p$, $E(\mathbb{Z}_r)$ is cyclic group for each $r \in \{p, q\}$. Assume that for a set $\mathbf{X}$, $0 \leq \eta \leq 1/2$ and for some (explicitly determined) constant $c = c(\vartheta)$, we have that $G_{B,\mathbf{X}}$ is cyclic and we have

$$|G_{\mathbf{X}}| \geq N^{1-\eta} \tag{14}$$

and

$$s_B(E_r) \geq c(\vartheta) r^{2\eta}. \tag{15}$$

Then the set $\mathbf{X}$ is (E, B)-separating set and in deterministic time $|\mathbf{X}| B^{2+o(1)}$ one can discover decomposition $N = pq$.

Separating sets, admissible curves and $(E, B, D)-$factoring

Let $B < D$, $\mathbf{X}$ be the (E, B, D)-separating set, $\beta \in [0, 1]$ and $0 \leq \gamma \leq \min(1 - \beta, 1/4)$.

- Let E over $\mathbb{Z}_N$ be either B-smooth or (B, β, D)-smooth.
  If E is (B, β, D)-smooth elliptic curve then some local order E_r is of type $E_r = s_B(E_r)\bar{q}$, where $\bar{q} > 1$ is composed of primes $l \in (B, D]$.
  The (E, B, D)-separating witness $\bar{P}$ for N has some local order $\mathrm{ord}P$ or $\mathrm{ord}P'$ of the type $m = s_B(m)\bar{q}$, where $\bar{q} \neq 1$.
- The significant role in the estimation of deterministic time factoring N is played by the following condition used in the definition of $(Y, \gamma)-$admissible elliptic curve E over $\mathbb{Z}_N$, namely that

$$1 \leq \min(a_E(p), a_E(q)) \leq c(\vartheta) N^{\frac{1}{4} - \frac{\gamma}{2}} \tag{16}$$

Result on $(E, B, D)-$factoring

Theorem 7 (Jurkiewicz, Pomykała, Prabucka, Żołnierczyk 2024)

Let $N = pq \geq N_0$ be sufficiently large, where $p < q < \vartheta p$ and $B < D \leq B^2$. Then we have

(i) *Let E be B-smooth elliptic curve over $\mathbb{Z}_N$ and $\bar{P}$ be (E, B)-separating witness for N. Then one can decompose N in deterministic time $B^{2+o(1)}$.*
If $\bar{P}$ is not (E, B)-separating witness then we have

$$\mathrm{ord}P = s_B(\mathrm{ord}P) = s_B(\mathrm{ord}P') = \mathrm{ord}P' = \mathrm{ord}\bar{P} \tag{17}$$

and one can factor N in additional deterministic time polylog$N$ provided for some $0 \leq \gamma < 1/4$ the equation (16) holds true and $\mathrm{ord}\bar{P} > N^{1/2-\gamma/2}$ (the last implies that E is (B, γ)- admissible elliptic curve).

Cont.

(ii) Let E be D-smooth elliptic curve. If $\mathbf{X}$ is (E, B, D) separating set then one can decompose $N = pq$ in **deterministic time** $|\bar{X}|(BD)^{1+o(1)}$, as $N \to \infty$. Moreover if the finite point $\bar{P} \in \mathbf{X}$ is $(E, B)-$ decomposition witness for N, then one can find the prime power representation of its order in deterministic time $B^{2+o(1)}$, as $N \to \infty$.

(iii) Let E be (B, β, D)-smooth elliptic curve. If $G_{\mathbf{X}} \subseteq E(\mathbb{Z}_N)$ is cyclic group, $|G_{\mathbf{X}}| \geq N^{1-\gamma}$ and $\mathbf{X}$ **is not** (E, D) separating set, then one can compute the generator $\bar{P}_0 \in G_{\mathbf{X}}$ such that at least one of local orders $\mathrm{ord}P_0$ **or** $\mathrm{ord}P_0'$ is **greater or equal** to $N^{1/2-\gamma/2}$, in **deterministic time** $|\mathbf{X}|BD^{1+o(1)}$, as $N \to \infty$.
Moreover, if

$$1 \leq \min(a_E(p), a_E(q)) \leq c(\vartheta)N^{\frac{1}{4}-\frac{\gamma}{2}} \tag{18}$$

then E must be (B, γ)-admissible and if $0 \leq \gamma < \min(1/4, 1-\beta)$, then one can **decompose** $N = pq$ in **deterministic time** $|\bar{X}|\mathrm{polylog}N$.

$(E,B,\beta,D,\sigma)-$factoring for subexponential B and D

Inspired by *Lenstra's* ECF method (**1987**) we can extend it for parameters $B = D^{\sigma/2}$, where $\sigma \in [1,2]$ and $\beta \leq \min\left(1, \sigma^2 \frac{\log B}{\log N}\right)$ to obtain the average-case time complexity that is not worse than Lenstra's $L(2\alpha_0 + o(1), r)$.
Namely let $B = L(\alpha, r) < D = L(\alpha_0, r)$, where $\alpha_0 = 1/\sqrt{2}$. The analysis of the distribution of D-smooth local orders E_r applies the condition $s_B(E_r) \geq E_r^{\beta}$ and that $(E_r/s_B(E_r))^*$ does not exceed D^{σ}.

Cont.

Counting the fraction of triples $T = (x, y, b_1) \in \mathbb{Z}_N^3$ such that the elliptic curve $E_{\bar{b}}$ over $\mathbb{Z}_N$ is $(I_r, B, \beta, D, \sigma)$-admissible, and assuming the conjecture that this fraction is equal

$$L^{-1}\left(\frac{1-\theta_\sigma(1-\beta)}{\sigma\alpha_0} + o(1),\ r\right).$$

one obtains the possible improvement of the **average-case time** complexity $L(2\alpha_0 + o(1), r)$ provided $\theta_\sigma \geq \frac{2-2\sigma+\sigma^2}{2(1-\sigma)}$ with the choice $B = D^{\sigma/2}$.

Schedule of presentation

- Preliminaries on elliptic curves over $\mathbb{Z}_N$ and partially smooth numbers
- Separating witnesses and separating sets
- **Multiplicative functions approach**
- Oracle factorization and rigorous approach

$f-$admissibility, classical example

Let f be a multiplicative function. The generalization of partially smooth numbers with respect to f are related to $f(n) = E_n$.

Definition 8

Let N be fixed. The positive integer m is called (f, B, β, D) or $(f, B, \beta, D, \sigma)-$admissible if $f(p)$ is (f, B, β, D) or $(f, B, \beta, D, \sigma)-$smooth number for some $p \mid N$.

Example. For $f(n)$ being the Euler $\phi(n)$ or divisor function $\sigma_k(n)$ the investigation were done by *Źrałek (***2010***), Bystrzycki, (***2018***)* concerning the deterministic time reduction of factorization problem to computing the above functions $f(n)$, respectively. The approaches were classical (without the application of elliptic curves). The second approach applied the additive combinatoric method.

Multiplicative functions approach

Let f be a multiplicative function. The general problem of deterministic factoring of $N \in \mathbb{N}_m$ to investigate the efficient factorization of N provided $f(N)$ is known, where $N \in \mathbb{N}_m$ ($m-$factoring) or $N \in \mathbb{N}$ (ordinary factoring).

- In general, the problem of deterministic polylog$N$ factoring is not within the reach of current methods except from the particular cases concerning f or m
- The reasonable weakening is to consider the tuple $\bar{f} = (f_1, f_2, ..., f_k)$ of multiplicative functions f_i and the tuple of positive integers $\bar{N} := (N_1, N_2, ..., N_h)$ such that $(f_i(N_j))_{i \leq k, j \leq h}$ are known.
- Particularly interesting cases are when k = 1 or h = 1 (when the vector of functions or arguments is trivial).

Towards the oracle factoring

- The values of $f_i(N)$ can be the iterations of the given function f in different points N_j
- The values $f(N_j)$ can be regarded as oracle querries
- Decomposition $N = pq$ provided for some α with $(\alpha/N) = -1$ we know both E_N and

$$E_N^\alpha := (p+1-a_{E^\alpha}(p))(q+1-a_{E^\alpha}(q)) =$$

$$= \left(p+1-\left(\frac{\alpha}{p}\right)a_E(p)\right)\left(q+1-\left(\frac{\alpha}{q}\right)a_E(q)\right).$$

- The above idea can be extended for arbitrary N provided we assume GRH (see below)

Factoring with probability $1-\varepsilon$

Lemma 9 (Lamzouri, Soundararajan (2015))

Let m be an integer and p a prime not dividing m. Assuming GRH, there exist $d \ll (\log mp)^2$ such that $\left(\frac{d}{p}\right) = -1$ and $\left(\frac{d}{m}\right) = 1$.

Now using the properties

$$E_N = \prod_{p|N} (p+1-a_p(E)),$$

$$E_N^d = \prod_{p|N} \left(p+1-\left(\frac{d}{p}\right) a_p(E)\right).$$

and writing the ratio E_N/E_N^d in irreducible form a/b we find the values pf $p+1-a_p(E)$ and $p+1+a_p(E)$ in deterministic time $D(polylog(N))$, provided $\gcd(p+1, a_p(E)) \leq D$. The last condition is fulfilled with probability $1-\varepsilon$ in view of result by *Lenstra (***1987***)*. We obtain

cont.- Result

Theorem 10 (*Jimenez Urroz, Pomykała*, 2023)

Let N be a squarefree integer. Then, assuming GRH, counting the number of points on elliptic curves modulo N allows to find the complete factorization of N with probability bigger than $1-\varepsilon$ for any $\varepsilon > 0$.

The randomized polynomial time follows with the choice $D = (\log N)^{O(1)}$.

Above we have applied the special case of the signature $sig(d, \mathscr{P})$ with exactly one term equal to -1, with $\mathscr{P}$ being the set of prime divisors of N defined by the sequence (in increasing order of primes coprime to d)

$$sig(d, \mathscr{P}) = \left(\left(\frac{d}{p} \right)_{p \in \mathscr{P}} \right).$$

and search for the elliptic curves satisfying the condition

$$\gcd(p+1, a_p(E)) \leq \Delta.$$

Rigorous approach and $(E, \Delta, p)-$exceptional numbers

The rigorous approach is looking for an algorithm algorithm $\mathscr{A}$ factoring almost all $N \leq x$ in deterministic time $t = polylog(N)$, unconditionally.

Definition 11

The squrefree number N is called $(E, \Delta, p)-$exceptional if $p \mid N$ and the condition $\gcd(p+1, a_p(E)) \leq \Delta$ does not hold.

Instead of the the assumption GRH we try to estimate the number of $N \leq x$ which are the $(E, D, p)-$exceptional for some $p \mid N$. This can be done by analytic number theory methods.

Signatures and patterns

For a finite set of primes $\mathscr{P}$ we define the classical signature as the following sequence

$$sig(d, \mathscr{P}) = \left(\frac{d}{p}\right)_{p \in \mathscr{P}}$$

with primes of $\mathscr{P}$ in increasing order. The special cases of $\mathscr{P}$ related to N play the significant role, namely $\mathscr{P}$ being the set of prime divisors of N.
Above the special role played the signatures with exactly one term equal to -1. In the following section we consider the analogous notion for elliptic curve E.

Definition 12

The sequence

$$S(E,\mathscr{P}) := \left(\left(\frac{a_p(E)}{p} \right)_{p\in\mathscr{P}} \right)$$

is called the elliptic signature (wrt. $\mathscr{P}$).

On the other hand an arbitrary sequence

$$S = S(\mathscr{P}) := (s_{p_1}, \cdots s_{p_k})$$

where $s_i \in (-2\sqrt{p_i}, 2\sqrt{p_i})$ for $p_i \in \mathscr{P}\,(i \leq k)$ is called the $\mathscr{P}-$pattern.

Lower bound for conductors N_E

Let Q be sufficiently large. We define the function $N(S,Q)$ counting the number of $q \leq Q$ for which there exist an elliptic curve $E = E_{\bar{b}}$ of conductor q and signature S. Let $\alpha = 0,1688...$ and P be the product of all primes $p \in \mathscr{P}$. We have

Theorem 13 (*Dąbrowski, Pomykała, Pujahari* **2022**)

Let ε be arbitrary (sufficiently small) positive constant. Assume that $P \leq \varepsilon Q^{1/3}$ and $S = S(\mathscr{P})$ be realizable by some elliptic curve $E = E_{\bar{b}}$ of minimal discriminant $|\Delta_E| \leq \varepsilon Q$. Then we have the lower bound

$$N(S,Q) \gg_{\varepsilon} \frac{Q^{5/6-\alpha}}{P^2}$$

This says that there are many elliptic curves $E = E_{\bar{b}}$ with bounded conductor $N_E \leq Q$ with the fixed signature $S(E,\mathscr{P}) = S$. The case of one-term signature is relating to the above condition $\gcd(p+1, a_p(E)) \leq \Delta$ and consequently to the distribution of $(E,\Delta,p)-$exceptional numbers above.

Examples of $f_i(N_j)$ sequences

Let $L(s,E)=\sum_n a_E(n)n^{-s}$ be the Hasse-Weil $L-$function of elliptic curve $E(\mathbb{Q})$. We let $f(N)=a_E(N)\neq 0$. Then the problem of factoring $N\in\mathbb{N}_m$ can be solved in deterministic polylog$N$ time provided we know the values of $f(N^j)$ for $j=1,2,...,m$. Here the essential tool is the recurrence formula

$$f(p^{\nu+1})=f(p)f(p^{\nu})-pf(p^{\nu-1})$$

(*Bach, Charles,* **2007,** *Chow,* **2015**). On the other hand, let N be coprime to $6\Delta_E$ and

$$f(N):=E_N=E_pE_q=(p+1-a_E(p))(q+1-a_E(q)),$$

where Δ_E is the minimal discriminant of $E(\mathbb{Q})$. Then N can be decomposed (conditionally) in polylog$N$ deterministic time (*Dieulefait, Urroz*, **2020** provided $\omega(E_N)$ is relatively small and *Pomykała, Żołnierczyk* **2024** *if* $\Omega(\gcd(E_p,E_q))$ *is relatively small).*

Separating primes and witnesses

Definition 14

The prime l is called $\bar{P}-$separating prime for N if

$$\nu_l(\mathrm{ord}P_p) \neq \nu_l(\mathrm{ord}P_q).$$

Alternatively we call $\bar{P}$ the $l-$separating witness for N

- The least $\bar{P}-$separating prime l, $(l \leq B)$ has played the significant role in the above discussion
- The particular case $l = 2$ is particularly interesting
- Also the application on the reduction of factoring N to the number of points on twists of superelliptic curves given by the affine equation $y^k = f(x_1, ..., x_d)$ is admissible *(Dryło, Pomykała* **2017***).*

2−adic separation, for $N \in \mathbb{N}_s$, probabilistic approach

The interesting question is to give the lower bound for the number of 2−separating witnesses for N. It is proved that the related fraction is $> 1/3$, namely we have

Theorem 15 (Dryło, Pomykała 2019)

Let $E/\mathbb{Z}_N$ be an elliptic curve with even order $|E(\mathbb{Z}_{p_i})|$ for some $1 \leq i \leq s$. Suppose that $\bar{P} \in E(\mathbb{Z}_N)$ satisfies

$$v_2(\mathrm{ord} P_i) \neq v_2(\mathrm{ord} P_j) \text{ for some } i, j, \tag{19}$$

where $\varphi(\bar{P}) = (P_1, \ldots, P_s)$. If $e_{\bar{P}}$ is an exponent of $\bar{P}$, then computing $e_{\bar{P}}$, using the double-and-add method we find a divisor of N in deterministic time $(\log N)^{1+o(1)}$, as $N \to \infty$ and we have

$$\#\{\bar{P} \in E(\mathbb{Z}_N) : \bar{P} \text{ satisfies (19)}\}/|E(\mathbb{Z}_N)| \geq \frac{27}{80} > \frac{1}{3}. \tag{20}$$

Counting functions and rigorous approach

- Oracle factoring represents the polynomial time reduction of factorization problem to computing the exponents of points $\bar{P} \in E(\mathbb{Z}_N)$ or the multiples of E_N.
- For a given algorithm A the function $F_I(x, t, A)$ counts the number of $N \leq x$, which are factored by A in deterministic time $\leq t$.
- Finding the algorithm A factoring the positive density of integers $N \in \mathbb{N}_I$, $N \leq x$ in polynomial time t that is to prove the lower bound

$$F_I(x, t, A) \geq N_I(x)(1 + o(1))$$

for $t = polylogN$ is beyond the reach of current methods (cf. *Knuth, Trabb-Pardo* **1976**, *Pomerance* **1982**, *Adleman, McCurley* **1987**, *Hafner-McCurley,* **1989**.)

Cont.

- For the analogous counting function the realistic is the asymptotics

$$F_I(x, t_A, A, O, t_A, t_O) = N_I(x)(1 + o(1))$$

as $N \to \infty$. The real problem here is to prove the asymptotics with relatively good error term for deterministic algorithm A where t_A and t_O are $(\log N)^{O(1)}$. For this we use the counting functions of smooth numbers $N \in \mathbb{N}_s$.

Evaluations of smooth numbers in $\mathbb{N}_s$

We have the following inequalities for y-smooth numbers $N \le x$, where $N \in \mathbb{N}_s$ (*Dryło-Pomykała,* **2019).**

Theorem 16

For arbitrary fixed integer $s \ge 2$, any $\theta \in (0,1)$, $c \in (0,1)$ and y satisfying the following condition

$$3 \le y \le \exp\left((\log x)^{\theta}\right) \tag{21}$$

we have

$$\begin{aligned} \frac{c}{2(s)!}\frac{x}{\log x}\Big((1-\theta)\log\log x\Big)^{s-1} &\le \#\mathbb{N}_s(x,y) \\ &\le \frac{1}{c(s-1)!}\frac{x}{\log x}(\log\log x)^{s-1}, \end{aligned} \tag{22}$$

where $x > x_0(c,\theta,s)$ is sufficiently large.

Twists of elliptic curves-failure set

Assuming we have the oracle *OrdEll* we need the upper bound for the set of numbers $N \in \mathbb{N}_s, N \leq x$, which are not factored in deterministic polylog$N$ time by the given algorithm A (called failure set).

It is related to the above approach with multiplicative functions $f_i(N) = \prod_{p|N}(p+1-a_E^{\alpha_i}(p))$, where $a_E^{\alpha_i} := a_E(p)\left(\frac{\alpha_i}{p}\right)$ and α_i are coprime to N.

The case of arbitrary $N \in \mathbb{N}$ is harder and is considered below.

Schedule of presentation

- Preliminaries on elliptic curves over $\mathbb{Z}_N$ and partially smooth numbers
- Separating witnesses and separating sets
- Multiplicative functions approach
- **Oracle factorization and rigorous approach**

MultEll (N, B, M)-oracle

First we describe a MultEll (N, B, M)-oracle which we assume is available to us. Let

$$E_b : y^2 = x(x^2 - b)$$

be an elliptic curve over $\mathbb{Z}_n$. By the Chinese remainder theorem we see that for a square-free n, the number of solutions $E(n, b)$ to the congruence

$$y^2 \equiv x(x^2 - b) \mod N, \qquad (x, y) \in \mathbb{Z}_n^2,$$

is given by

$$E(n, b) = \prod_{p|n} \#(E_b(\mathbb{Z}_p)), \tag{23}$$

provided that $\gcd(b, n) = 1$,

MultEll (N, B, M)-oracle, cont.

Definition 17 (MultEll(N, B, M)-oracle)

Given the parameters B, N and M, for each integer $n \leq N$ it returns

- a positive multiple

$$k_b E(N, b) \leq M, \qquad k_b \in \mathbb{N},$$

  of $E(n, b)$ given for every $b \leq B$ with $\gcd(b, n) = 1$, if n square-free
- an error message $\star\star\star$, if N is not square-free.

Theorem 18 (*Dąbrowski, Pomykała, Shparlinski,* **2023**)

Let

$$2 < \gamma < 2 + \frac{\sqrt{257} - 15}{16}\delta < 1/4$$

be fixed. Assume that for a sufficiently large integer N we are given a MultEll (N, B, M)-oracle where

$$B = (\log N)^{\gamma},\ M = N^{O(1)}$$

Then there is a ***deterministic algorithm*** *that finds a nontrivial factor of all integers $n \leq N$ with at most $N/(\log N)^{\delta}$ exceptions, in polynomial, deterministic time $O((\log N)^{\rho(\gamma)+o(1)})$, where*

$$\rho(\gamma) = \max\left\{\gamma + 2, \frac{9\gamma - 17}{8(\gamma - 2)}\right\}$$

and $O((\log N)^{\gamma})$ oracle queries.

Definition 19 (MultEll$^*(N, B, M)$-oracle)

Given the parameters B, N and M, for each $N \leq N$, it returns

- a positive multiple

$$kF(n, B) \leq M, \qquad k \in \mathbb{N},$$

of

$$F(n, B) = \prod_{b \leq B} E(n, b),$$

if n is square-free;

- an error message $\star\star\star$, if n is not square-free.

Theorem 20 (*Dąbrowski, Pomykała, Shparlinski,* **2023**)

There are some positive constants c and C such that if for a sufficiently large integer N we are given a (N, B, M)-oracle, where

$$B = c \log NM = N^{O(B)},$$

then ***there is*** *a* ***deterministic algorithm*** *that finds a nontrivial factor of all integers $n \le N$ with at most $N(\log N)^{-C/\log\log\log N}$ exceptions, in polynomial, deterministic time $\log^{3+o(1)} N$, with only one query of the MultEll* (N, B, M)-oracle.*

Oracle's parameters

- The parameter γ controls the size of B ($B \leq (\log N)^{\gamma}$) and the preliminary sieving by the small primes $p \in [\log N, \exp(\log N)^{\delta}]$, where $0 \leq \delta < 1/4$). Moreover $M \leq N^{O(1)}$.
- In the second theorem $B = O(\log N)$ and $M = N^{O(B)}$.

Thank You

jacek.pomykala@wat.edu.pl; pomykala@mimuw.edu.pl