

MULTIPLE BASE DISCRETE LOGARITHM PROBLEM

Grzegorz Banaszak & Dorota Blinkiewicz

Adam Mickiewicz University in Poznań

NuTMiC 2026:
Number-Theoretic Methods in Cryptology
Katowice, September 21–23, 2026

Discrete logarithm problem (see [CP, Chapters 5, 6], [SP, Chapter 7]): problem concerning solutions of the equation $a^x = b$ with $a, b \in \mathbb{F}_p^\times$.

Discrete logarithm problem can be extended to any abelian group G : it concerns solutions of $g_1^x = g$ in $x \in \mathbb{Z}$, where $g_1, g \in G$.

Natural generalization of discrete logarithm problem to multiple base $(\alpha_1, \dots, \alpha_n)$.

A multiple base $(g_1, \dots, g_n)$ discrete logarithm problem in an abelian group G concerns solutions of

$$g_1^{x_1} \cdot \dots \cdot g_n^{x_n} = g \text{ in } (x_1, \dots, x_n) \in \mathbb{Z}^n,$$

where $g_1, \dots, g_n, g \in G$.

Notation:

Let

- F be a number field,
- $\mathcal{O}_F$ the ring of integers in F ,
- S be a finite set of prime ideals of $\mathcal{O}_F$,
- $\mathcal{O}_{F,S}$ be the ring of S -integers,
- $\mathbb{G}_m$ denotes the multiplicative group scheme.

REMARK

For any commutative ring R , its R -valued points $\mathbb{G}_m(R)$ correspond to the group of units, i.e., $\mathbb{G}_m(R) = R^\times$.

Because of number of technical computations we will keep working with $F = \mathbb{Q}$ and $\mathcal{O}_F = \mathbb{Z}$ for simplicity of presentation.

(*) Our computations can easily be extended to $\mathcal{O}_{F,S}$, for any number field F , with S such that $\mathcal{O}_{F,S}$ is a PID.

For this reason this introduction is presented in the general form for any number field F .

In relation to the discrete logarithm problem in $\mathbb{F}_p^\times$ there is an important **local to global discrete logarithm problem**.

It asks:

whether equation

$$\alpha^x = \beta \text{ in } \mathcal{O}_{F,S}^\times$$

has solution in $x \in \mathbb{Z}$ if and only if equation

$$r_v(\alpha)^{x_v} = r_v(\beta) \text{ in } k_v^\times$$

has solution in $x_v \in \mathbb{Z}$ for almost all prime ideals $v \in \mathcal{O}_{F,S}$,
where $r_v : \mathcal{O}_{F,S}^\times \rightarrow k_v^\times$ is the reduction map at v .

This problem was solved affirmatively by A. Schinzel in 1975 [Sch, Theorem 2, p. 398].

One can consider natural generalization of **the local to global discrete logarithm problem to multiple base** $(\alpha_1, \dots, \alpha_n)$.

However, here situation is not as simple as for the single base local to global discrete logarithm problem.

Namely,

- A. Schinzel [Sch, pp. 419-420] gave counterexample to multiple base discrete logarithm problem in $\mathbb{G}_m^2(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}])$.
- in [BK, pp. 330-332], the Schinzel's counterexample [Sch, pp. 419-420] was extended to abelian surfaces E_d^2 , where E_d is the CM elliptic curve given by the equation $y^2 = x^3 - d^2x$ for $d \in \mathbb{Z}$.
- in [BB, pp. 149-152], the Schinzel's counterexample was generalized to $\mathbb{G}_m^2(\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{5}])$.
- etc.

Aim of the lecture:

we show that **the local to global multiple base $(\alpha_1, \dots, \alpha_n)$ discrete logarithm problem in $\mathbb{G}_m^2(\mathcal{O}_{F,S}) = (\mathcal{O}_{F,S}^\times)^2$ has counterexamples for arbitrary big bases, including infinite bases** (Theorem 2.2 cf. Remark 2.1, Corollaries 2.6, 3.1).

Let $n \in \mathbb{N}$, $n \geq 3$.

Let $p_1, p_2, \dots, p_n$ be different prime numbers.

Let $F = \mathbb{Q}$ and $S = \{p_1, p_2, \dots, p_n\}$ then $\mathbb{Z}_S = \mathbb{Z}[\frac{1}{p_1}, \frac{1}{p_2}, \dots, \frac{1}{p_n}]$.

Consider the group scheme $\mathbb{G}_m^2 := \mathbb{G}_m \times_{\text{spec } \mathbb{Z}_S} \mathbb{G}_m$.

Let N, N' be arbitrary positive integer numbers.

Consider the following elements in $\mathbb{G}_m^2(\mathbb{Z}_S) = \mathbb{Z}_S^\times \times \mathbb{Z}_S^\times$:

$$\begin{aligned} \lambda &= \begin{bmatrix} 1 \\ p_1^N \end{bmatrix}, \lambda_1 = \begin{bmatrix} p_1 \\ 1 \end{bmatrix}, \lambda_2 = \begin{bmatrix} p_2 \\ p_1 \end{bmatrix}, \lambda_3 = \begin{bmatrix} p_3 \\ p_2 \end{bmatrix}, \dots, \\ \lambda_{n-1} &= \begin{bmatrix} p_{n-1} \\ p_{n-2} \end{bmatrix}, \lambda_n = \begin{bmatrix} p_n \\ p_{n-1} \end{bmatrix}, \lambda_{n+1} = \begin{bmatrix} 1 \\ p_n \end{bmatrix}, \lambda' = \begin{bmatrix} p_n^{N'} \\ 1 \end{bmatrix}. \end{aligned} \tag{2.1}$$

Consider the following subgroups of $\mathbb{Z}_S^\times \times \mathbb{Z}_S^\times$:

$$\begin{aligned}\Lambda &:= \lambda^{\mathbb{Z}} \cdot \lambda_1^{\mathbb{Z}} \cdot \lambda_2^{\mathbb{Z}} \cdot \lambda_3^{\mathbb{Z}} \cdot \dots \cdot \lambda_n^{\mathbb{Z}} \cdot \lambda_{n+1}^{\mathbb{Z}}, \\ \Lambda' &:= \lambda_1^{\mathbb{Z}} \cdot \lambda_2^{\mathbb{Z}} \cdot \lambda_3^{\mathbb{Z}} \cdot \dots \cdot \lambda_n^{\mathbb{Z}} \cdot \lambda_{n+1}^{\mathbb{Z}} \cdot \lambda'^{\mathbb{Z}}.\end{aligned}\tag{2.2}$$

REMARK 2.1

Observe that $\lambda, \lambda_1, \lambda_2, \dots, \lambda_{n+1}, \lambda'$ are linearly independent over $\mathbb{Z}$ in $\mathbb{Z}_S^\times \times \mathbb{Z}_S^\times$, so $\lambda, \lambda' \notin \Lambda \cap \Lambda'$ and:

$$\begin{aligned}\Lambda \cap \Lambda' &= \lambda_1^{\mathbb{Z}} \cdot \lambda_2^{\mathbb{Z}} \cdot \lambda_3^{\mathbb{Z}} \cdot \dots \cdot \lambda_n^{\mathbb{Z}} \cdot \lambda_{n+1}^{\mathbb{Z}}, \\ \Lambda \cdot \Lambda' &= \lambda^{\mathbb{Z}} \cdot \lambda_1^{\mathbb{Z}} \cdot \lambda_2^{\mathbb{Z}} \cdot \lambda_3^{\mathbb{Z}} \cdot \dots \cdot \lambda_n^{\mathbb{Z}} \cdot \lambda_{n+1}^{\mathbb{Z}} \cdot \lambda'^{\mathbb{Z}}.\end{aligned}$$

Hence

$$\mathrm{rk}_{\mathbb{Z}} \Lambda = \mathrm{rk}_{\mathbb{Z}} \Lambda' = n + 2,\tag{2.3}$$

$$\mathrm{rk}_{\mathbb{Z}} \Lambda \cap \Lambda' = n + 1 \quad \text{and} \quad \mathrm{rk}_{\mathbb{Z}} \Lambda \cdot \Lambda' = n + 3.\tag{2.4}$$

THEOREM 2.2

For each $p \notin S$, let

$$r_p \times r_p : \mathbb{Z}_S^\times \times \mathbb{Z}_S^\times \rightarrow \mathbb{F}_p^\times \times \mathbb{F}_p^\times$$

be the reduction map (to make notation simple we will write r_p instead of $r_p \times r_p$).

Then for all $p \notin S$:

$$r_p(\lambda) \in r_p(\Lambda \cap \Lambda') \quad \text{and} \quad r_p(\lambda') \in r_p(\Lambda \cap \Lambda').$$

Sketch of the proof of Theorem 2.2:

Let $p \notin S$.

Let $\overline{\lambda} := r_p(\lambda)$, $\overline{\lambda'} := r_p(\lambda')$ and $\overline{\lambda_i} := r_p(\lambda_i)$ for $i = 1, \dots, n+1$.

The equation

$$\overline{\lambda} = \overline{\lambda_1}^{R_1} \overline{\lambda_2}^{R_2} \overline{\lambda_3}^{R_3} \dots \overline{\lambda_{n+1}}^{R_{n+1}} \quad (2.5)$$

is equivalent to the system of equations:

$$\begin{aligned} 1 &\equiv p_1^{R_1} p_2^{R_2} \dots p_n^{R_n} \pmod{p}, \\ p_1^N &\equiv p_1^{R_2} p_2^{R_3} \dots p_n^{R_{n+1}} \pmod{p}. \end{aligned} \quad (2.6)$$

For example:

Let $S = \{31, 3, 5\}$ and $p = 11 \notin S$. Then:

$$\lambda = \begin{bmatrix} 1 \\ 31^N \end{bmatrix}, \lambda_1 = \begin{bmatrix} 31 \\ 1 \end{bmatrix}, \lambda_2 = \begin{bmatrix} 3 \\ 31 \end{bmatrix}, \lambda_3 = \begin{bmatrix} 5 \\ 3 \end{bmatrix}, \lambda_4 = \begin{bmatrix} 1 \\ 5 \end{bmatrix}, \lambda' = \begin{bmatrix} 5^{N'} \\ 1 \end{bmatrix}.$$

Let $\overline{\lambda} := r_{11}(\lambda)$, $\overline{\lambda}' := r_{11}(\lambda')$ and $\overline{\lambda}_i := r_{11}(\lambda_i)$ for $i = 1, 2, 3, 4$.

The equation:

$$\overline{\lambda} = \overline{\lambda}_1^{R_1} \overline{\lambda}_2^{R_2} \overline{\lambda}_3^{R_3} \overline{\lambda}_4^{R_4}$$

is equivalent to the system of congruences:

$$\begin{cases} 1 \equiv 31^{R_1} 3^{R_2} 5^{R_3} \pmod{11} \\ 31^N \equiv 31^{R_2} 3^{R_3} 5^{R_4} \pmod{11} \end{cases} \iff \begin{cases} 1 \equiv 9^{R_1} 3^{R_2} 5^{R_3} \pmod{11} \\ 9^N \equiv 9^{R_2} 3^{R_3} 5^{R_4} \pmod{11} \end{cases}$$

Let g be a generator of $(\mathbb{Z}/p)^\times$, i.e.:

$$(\mathbb{Z}/p)^\times = \langle g \rangle.$$

Obviously $(\mathbb{Z}/p)^\times$ is isomorphic to $\mathbb{Z}/(p-1)$. Therefore, the system of equations (2.6) is equivalent to the system:

$$\begin{aligned} 0 &\equiv c_1 R_1 + c_2 R_2 + \dots + c_n R_n \pmod{p-1}, \\ Nc_1 &\equiv c_1 R_2 + c_2 R_3 + \dots + c_n R_{n+1} \pmod{p-1}, \end{aligned} \tag{2.7}$$

where

$$p_1 = g^{c_1}, p_2 = g^{c_2}, \dots, p_n = g^{c_n}$$

for some $c_1, c_2, \dots, c_n \in \mathbb{Z}/(p-1)$.

Let $g = 2$ be a generator of $(\mathbb{Z}/11)^\times$, i.e.:

$$(\mathbb{Z}/11)^\times = \langle 2 \rangle.$$

Define the isomorphism $(\mathbb{Z}/11)^\times \rightarrow \mathbb{Z}/10$ as follows $2^y \mapsto y$. Then:

$$9 = 2^6, 3 = 2^8, 5 = 2^4 \implies c_1 = 6, c_2 = 8, c_3 = 4.$$

Therefore:

$$\begin{cases} 1 \equiv 9^{R_1} 3^{R_2} 5^{R_3} \pmod{11} \\ 9^N \equiv 9^{R_2} 3^{R_3} 5^{R_4} \pmod{11} \end{cases} \iff \begin{cases} 0 \equiv 6R_1 + 8R_2 + 4R_3 \pmod{10} \\ 6N \equiv 6R_2 + 8R_3 + 4R_4 \pmod{10} \end{cases}$$

REMARK

For $p \notin S$ we may have two cases:

- ① $c_i \not\equiv 0 \pmod{p-1}$ for all $i = 1, \dots, n$;
- ② exists $i = 1, \dots, n$ such that $c_i \equiv 0 \pmod{p-1}$.

Case 1.

Assume that: $c_i \not\equiv 0 \pmod{p-1}$ for all $i = 1, \dots, n$.

We produce the auxiliary equation with integer coefficients:

$$\frac{c_1^2}{D_0}x_2 + \frac{c_1c_2}{D_0}x_3 + \dots + \frac{c_1c_{n-1}}{D_0}x_n + c_nR_{n+1} = Nc_1,$$

where

$$D_0 := \gcd(c_1, c_2, \dots, c_n).$$

We can prove that the above equation has integer solution:

$$(x_2, x_3, \dots, x_n, R_{n+1}) = (r_2, r_3, \dots, r_n, r_{n+1}).$$

Putting

$$R_1 = -\frac{c_2}{D_0}r_2 - \frac{c_3}{D_0}r_3 - \dots - \frac{c_n}{D_0}r_n,$$

$$R_2 = \frac{c_1}{D_0}r_2,$$

$$R_3 = \frac{c_1}{D_0}r_3,$$

$$\vdots$$

$$R_n = \frac{c_1}{D_0}r_n,$$

$$R_{n+1} = r_{n+1}$$

we observe, by simple computation, that $R_1, R_2, \dots, R_{n+1}$ satisfy the system of congruences (2.7).

$$\begin{cases} 0 \equiv 6R_1 + 8R_2 + 4R_3 \pmod{10} \\ 6N \equiv 6R_2 + 8R_3 + 4R_4 \pmod{10} \end{cases}$$

We see that for every $i = 1, 2, 3$: $c_i \not\equiv 0 \pmod{10}$.

We compute:

$$D_0 = \gcd(c_1, c_2, c_3) = \gcd(6, 8, 4) = 2.$$

We introduce the auxiliary equation:

$$\frac{c_1^2}{D_0}x_2 + \frac{c_1c_2}{D_0}x_3 + c_3R_4 = Nc_1 \iff 18x_2 + 24x_3 + 4R_4 = 6N.$$

Let

$$D = \gcd\left(\frac{c_1^2}{D_0}, \frac{c_1c_2}{D_0}, c_3\right) = \gcd(18, 24, 4) = 2.$$

Notice that $D|c_1 \iff 2|6$.

The equation:

$$18x_2 + 24x_3 + 4R_4 = 6N$$

has integer solutions:

$$\begin{cases} x_2 = N + 2a \\ x_3 = b \\ R_4 = -3N - 9a - 6b, \quad a, b \in \mathbb{Z}. \end{cases}$$

Taking $a = b = 0$, we get:

$$\begin{cases} R_1 = -\frac{c_2}{D_0}x_2 - \frac{c_3}{D_0}x_3 = -4N \\ R_2 = \frac{c_1}{D_0}x_2 = 3N \\ R_3 = \frac{c_1}{D_0}x_3 = 0 \\ R_4 = -3N. \end{cases}$$

Case 2.

Let us recall the system of congruences (2.7):

$$\begin{aligned}0 &\equiv c_1 R_1 + c_2 R_2 + \dots + c_n R_n \pmod{p-1} \\ Nc_1 &\equiv c_1 R_2 + c_2 R_3 + \dots + c_n R_{n+1} \pmod{p-1}\end{aligned}$$

Let $j \in \{1, 2, \dots, n\}$ be the smallest number such that

$$c_j \equiv 0 \pmod{p-1}.$$

- If $j = 1$ then we have the following solution:

$$(R_1, R_2, R_3, \dots, R_n, R_{n+1}) = (0, 0, 0, \dots, 0, 0).$$

- If $j = 2$ then we have the following solution:

$$(R_1, R_2, R_3, R_4, \dots, R_n, R_{n+1}) = (0, N, 0, 0, \dots, 0, 0).$$

- If $j \in \{3, \dots, n\}$ then set $R_i = 0$ for all $j + 1 \leq i \leq n + 1$.

Then we obtain the following congruences instead of (2.7):

$$\begin{aligned} 0 &\equiv c_1 R_1 + c_2 R_2 + \dots + c_{j-1} R_{j-1} \pmod{p-1} \\ Nc_1 &\equiv c_1 R_2 + c_2 R_3 + \dots + c_{j-1} R_j \pmod{p-1}. \end{aligned} \tag{2.8}$$

To obtain solution of (2.8) replace n by $j - 1$ in (2.7) and apply all operations from case 1 with this replacement.

Now, we should prove that $\overline{\lambda'} \in r_p(\Lambda \cap \Lambda')$. The equation:

$$\overline{\lambda'} = \overline{\lambda_1}^{R_{n+1}} \overline{\lambda_2}^{R_n} \overline{\lambda_3}^{R_{n-1}} \dots \overline{\lambda_{n+1}}^{R_1} \quad (2.9)$$

is equivalent to the system of congruences:

$$\begin{aligned} 1 &\equiv p_n^{R_1} p_{n-1}^{R_2} \dots p_1^{R_n} \pmod{p}, \\ p_n^{N'} &\equiv p_n^{R_2} p_{n-1}^{R_3} \dots p_1^{R_{n+1}} \pmod{p}. \end{aligned} \quad (2.10)$$

Observe that the systems of congruences (2.6) and (2.10) are basically the same (we have N' in place of N).

Observe that computations concerning solutions of (2.6) do not depend on N . Hence using the same computations we obtain a solution $R_1, R_2, R_3, \dots, R_{n+1}$ of (2.10).



COROLLARY 2.3

For each prime number $p \notin S$ we have the following equality:

$$r_p(\Lambda) = r_p(\Lambda') = r_p(\Lambda \cap \Lambda') = r_p(\Lambda \cdot \Lambda').$$

REMARK 2.4

For any set of different prime numbers $S = \{p_1, p_2, \dots, p_n\}$ we can find such natural numbers N, N' that system of congruences (2.6), (2.10) will have solutions also for $p \in S$. Indeed, let $N = N' := \varphi(p_1 p_2 \dots p_n)$, where $\varphi(\cdot)$ is the Euler's totient function. Then we obtain the following solutions:

	solutions of (2.6) modulo p_i ($R_1, R_2, R_3, \dots, R_n, R_{n+1}$)
$i = 1$	(0, $\varphi(p_1)$, 0, ..., 0, 0)
$i \neq 1$	(0, 0, 0, ..., 0, 0)

	solutions of (2.10) modulo p_i ($R_1, R_2, R_3, \dots, R_n, R_{n+1}$)
$i = n$	(0, $\varphi(p_n)$, 0, ..., 0, 0)
$i \neq n$	(0, 0, 0, ..., 0, 0)

REMARK 2.5

Let $N = N' = \varphi(p_1 p_2 \dots p_n)$. By Theorem 2.2 and Remark 2.4, multiple base $(\lambda_1, \dots, \lambda_{n+1})$ discrete logarithm of the elements λ and λ' has solutions modulo p , for all prime numbers p . However, multiple base $(\lambda_1, \dots, \lambda_{n+1})$ discrete logarithm of λ and λ' does not have solutions.

(*)

Our computations can easily be extended to $\mathbb{G}_m^2$ over $\mathcal{O}_{F,S}$, for any number field F , with S such that $\mathcal{O}_{F,S}$ is a PID.

This is because in a PID every non-zero prime ideal is maximal.

In the case when $\mathcal{O}_{F,S}$ is a PID, reducing modulo a non-zero prime ideal yields a finite field $\mathbb{F}_q$. Since the multiplicative group $\mathbb{F}_q^\times$ is cyclic, choosing a generator allows us to take discrete logarithm and induce an isomorphism with $\mathbb{Z}/(q-1)$. By passing to the exponents, the problem reduces to solving a similar system of two congruences, making the remaining part of proof entirely analogous to the case of $F = \mathbb{Q}$.

Let $S_1, \dots, S_t$ be a sequence of pairwise disjoint sets of prime numbers, i.e.:

$$S_j := \{p_{1j}, \dots, p_{n_jj}\},$$

such that $n_j > 2$ for each j . For fixed j , let $N_j, N'_j \in \mathbb{N}$.

In the same way as above, consider the following elements in $\mathbb{G}_m^2(\mathbb{Z}_{S_j}) = \mathbb{Z}_{S_j}^\times \times \mathbb{Z}_{S_j}^\times$:

$$\lambda_j = \begin{bmatrix} 1 \\ p_{1j}^{N_j} \end{bmatrix}, \lambda_{1j} = \begin{bmatrix} p_{1j} \\ 1 \end{bmatrix}, \lambda_{2j} = \begin{bmatrix} p_{2j} \\ p_{1j} \end{bmatrix}, \lambda_{3j} = \begin{bmatrix} p_{3j} \\ p_{2j} \end{bmatrix}, \dots,$$

$$\lambda_{(n_j-1)j} = \begin{bmatrix} p_{(n_j-1)j} \\ p_{(n_j-2)j} \end{bmatrix}, \lambda_{n_jj} = \begin{bmatrix} p_{n_jj} \\ p_{(n_j-1)j} \end{bmatrix}, \lambda_{(n_j+1)j} = \begin{bmatrix} 1 \\ p_{n_jj} \end{bmatrix}, \lambda'_j = \begin{bmatrix} p_{n_jj}^{N'_j} \\ 1 \end{bmatrix}.$$

Consider the following subgroups of $\mathbb{Z}_{S_j}^\times \times \mathbb{Z}_{S_j}^\times$:

$$\begin{aligned}\Lambda_j &:= \lambda_j^{\mathbb{Z}} \cdot \lambda_{1j}^{\mathbb{Z}} \cdot \lambda_{2j}^{\mathbb{Z}} \cdot \lambda_{3j}^{\mathbb{Z}} \cdot \dots \cdot \lambda_{n_j j}^{\mathbb{Z}} \cdot \lambda_{(n_j+1)j}^{\mathbb{Z}}, \\ \Lambda'_j &:= \lambda_{1j}^{\mathbb{Z}} \cdot \lambda_{2j}^{\mathbb{Z}} \cdot \lambda_{3j}^{\mathbb{Z}} \cdot \dots \cdot \lambda_{n_j j}^{\mathbb{Z}} \cdot \lambda_{(n_j+1)j}^{\mathbb{Z}} \cdot \lambda_j'^{\mathbb{Z}}.\end{aligned}\tag{2.11}$$

Let

$$\Sigma_t := \bigsqcup_{j=1}^t S_j.\tag{2.12}$$

Let

$$\begin{aligned}\Gamma_t &:= \Lambda_1 \cdot \dots \cdot \Lambda_t, \\ \Gamma'_t &:= \Lambda'_1 \cdot \dots \cdot \Lambda'_t\end{aligned}\tag{2.13}$$

be subgroups of $\mathbb{G}_m^2(\mathbb{Z}_{\Sigma_t}) = \mathbb{Z}_{\Sigma_t}^\times \times \mathbb{Z}_{\Sigma_t}^\times$.

Observe that:

$$\Gamma_t \cap \Gamma'_t = (\Lambda_1 \cap \Lambda'_1) \cdot \dots \cdot (\Lambda_t \cap \Lambda'_t),$$

$$\Gamma_t \cdot \Gamma'_t = \Lambda_1 \cdot \Lambda'_1 \cdot \dots \cdot \Lambda_t \cdot \Lambda'_t.$$

Notice also that:

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_t = \mathrm{rk}_{\mathbb{Z}} \Gamma'_t = \sum_{j=1}^t (n_j + 2),$$

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_t \cap \Gamma'_t = \sum_{j=1}^t (n_j + 1),$$

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_t \cdot \Gamma'_t = \sum_{j=1}^t (n_j + 3)$$

and

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_t / (\Gamma_t \cap \Gamma'_t) = \mathrm{rk}_{\mathbb{Z}} \Gamma'_t / (\Gamma_t \cap \Gamma'_t) = t. \quad (2.14)$$

COROLLARY 2.6

For each prime number $p \notin \Sigma_t$, we have the following equality:

$$r_p(\Gamma_t) = r_p(\Gamma'_t) = r_p(\Gamma_t \cap \Gamma'_t) = r_p(\Gamma_t \cdot \Gamma'_t).$$

REMARK 2.7

Let $N_j = N'_j = \varphi(p_{1j}p_{2j} \dots p_{n_jj})$ for each $j = 1, \dots, t$. Consider sequence b_t which is the concatenation of the sequences $(\lambda_{1j}, \dots, \lambda_{n_jj})$ for $j = 1, \dots, t$. By Theorem 2.2 and Remark 2.4, multiple base b_t discrete logarithm of each λ_j and λ'_j , $j = 1, \dots, t$, has solutions modulo p , for every p . However, multiple base b_t discrete logarithm of each λ_j and λ'_j , $j = 1, \dots, t$, does not have solutions.

Let $\mathcal{P} := \{2, 3, 5, \dots, p, \dots\}$ be the set of all prime numbers. Consider now infinite sequence of pairwise disjoint sets of prime numbers:

$$S_1 = \{p_{11}, \dots, p_{n_11}\}, \dots, S_t = \{p_{1t}, \dots, p_{n_t t}\}, \dots \quad (3.1)$$

Define $\Sigma_t := \bigsqcup_{j=1}^t S_j$ as in (2.12) and put

$$\Sigma_\infty := \bigcup_{t=1}^{\infty} \Sigma_t = \bigsqcup_{t=1}^{\infty} S_t.$$

Define subgroups Γ_t, Γ'_t of $\mathbb{G}_m^2(\mathbb{Z}_{\Sigma_\infty}) = \mathbb{Z}_{\Sigma_\infty}^\times \times \mathbb{Z}_{\Sigma_\infty}^\times$ as in (2.13).

Observe that:

$$\Gamma_1 \subset \dots \subset \Gamma_t \subset \Gamma_{t+1} \subset \dots,$$

$$\Gamma'_1 \subset \dots \subset \Gamma'_t \subset \Gamma'_{t+1} \subset \dots$$

Let

$$\Gamma_{\infty} := \varinjlim_t \Gamma_t = \bigcup_{t=1}^{\infty} \Gamma_t,$$
$$\Gamma'_{\infty} := \varinjlim_t \Gamma'_t = \bigcup_{t=1}^{\infty} \Gamma'_t.$$

Notice that

$$\Gamma_{\infty} \cap \Gamma'_{\infty} = \varinjlim_t \Gamma_t \cap \Gamma'_t = \bigcup_{t=1}^{\infty} \Gamma_t \cap \Gamma'_t$$

and

$$\Gamma_{\infty} \cdot \Gamma'_{\infty} = \varinjlim_t \Gamma_t \cdot \Gamma'_t = \bigcup_{t=1}^{\infty} \Gamma_t \cdot \Gamma'_t.$$

Observe that

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_{\infty} = \mathrm{rk}_{\mathbb{Z}} \Gamma'_{\infty} = \mathrm{rk}_{\mathbb{Z}} \Gamma_{\infty} \cap \Gamma'_{\infty} = \mathrm{rk}_{\mathbb{Z}} \Gamma_{\infty} \cdot \Gamma'_{\infty} = \infty$$

and

$$\mathrm{rk}_{\mathbb{Z}} \Gamma_{\infty} / (\Gamma_{\infty} \cap \Gamma'_{\infty}) = \mathrm{rk}_{\mathbb{Z}} \Gamma'_{\infty} / (\Gamma_{\infty} \cap \Gamma'_{\infty}) = \infty.$$

COROLLARY 3.1

Assume that $\mathcal{P} \setminus \Sigma_{\infty} \neq \emptyset$. For each prime number $p \notin \Sigma_{\infty}$, we have the following equality:

$$r_p(\Gamma_{\infty}) = r_p(\Gamma'_{\infty}) = r_p(\Gamma_{\infty} \cap \Gamma'_{\infty}) = r_p(\Gamma_{\infty} \cdot \Gamma'_{\infty}).$$

REMARK 3.2

Let $N_j = N'_j = \varphi(p_{1j}p_{2j} \dots p_{n_{jj}})$ for each $j \in \mathbb{N}$. Consider sequence b_∞ which is the concatenation of the sequences $(\lambda_{1j}, \dots, \lambda_{n_{jj}})$ for $j \in \mathbb{N}$. By Theorem 2.2 and Remark 2.4, multiple base b_∞ discrete logarithm of each λ_j and λ'_j , $j \in \mathbb{N}$, has solutions modulo p , for every p . However, multiple base b_∞ discrete logarithm of each λ_j and λ'_j , $j \in \mathbb{N}$, does not have solutions.

REMARK 3.3

Observe that Remark 3.2 works also in the case where $\Sigma_\infty = \mathcal{P}$. In this case $\mathbb{Z}_{\Sigma_\infty} = \mathbb{Q}$ but the reader observes that it is not an obstruction to run down our computations.

REFERENCES I

-  G. Banaszak, D. Blinkiewicz, *Commensurability in Mordell-Weil groups of abelian varieties and tori*, *Functiones et Approximatio* **58** no. 2, (2018), 145-156.
-  G. Banaszak, P. Krasoń, *On arithmetic in Mordell-Weil groups*, *Acta Arithmetica* **150** no. 4, (2011), 315-337.
-  R. Crandall, C. Pomerance, *Prime Numbers. A Computational Perspective. Second Edition*, Springer Science+Business Media, Inc., USA (2005).
-  K. Rubin and A. Silverberg, *Ranks of elliptic curves*, *Bull. Amer. Math. Soc.* **39** (2002), 455-474.
-  A. Schinzel, *On power residues and exponential congruences*, *Acta Arithmetica* **27**, (1975), 397-420.

REFERENCES II



D.R. Stinson, M.B. Paterson, *Cryptography: Theory and practice. Fourth Edition*, Textbooks in Mathematics, CRC Press, Taylor & Francis Group, (2019).