Principles of geometric correlation in the construction of models of multifactorial situations and processes/ Adoniev Y., Vereshchaga V. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 19 (1241).– P.48–53. – Bibliogr.:10. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Верещага Віктор Михайлович – доктор технічних наук, професор кафедри прикладної математики та інформаційних технологій Мелітопольського державного педагогічного університету ім. Богдана Хмельницького; вул. Гетьманська, 20, м. Мелітополь, Україна, 72300; e-mail: vervik49@gmail.com.

Адоньев Евгений Александрович – кандидат технических наук, доцент, декан Экономико-гуманитарного факультета Запорожского национального университета в г. Мелитополе; ул. Героев Украины, 160А, г. Мелитополь, Украина, 72316, e-mail: evgen.adoniev@gmail.com.

Верещага Виктор Михайлович – доктор технических наук, профессор кафедры прикладной математики и информационных технологий Мелитопольського государственного педагогического университета им. Богдана Хмельницкого; ул. Гетьманская, 20, г. Мелитополь, Украина, 72300; , e-mail: vervik49@gmail.com.

Adoniev Yevhen – PhD, associate professor, dean of the Economics and Humanities Faculty of the Zaporizhzhya National University in Melitopol. Heroiv Ukrainy str., 160A, Melitopol, Ukraine, 72316; e-mail: evgen.adoniev@gmail.com.

Vereshchaga Viktor – Doctor of Technical Sciences, Professor of the Department of Applied Mathematics and Information Technologies of the Melitopol State Pedagogical University named after Bohdan Khmelnytsky; Getmansky str., 20, Melitopol, Ukraine, 72300;, e-mail: vervik49@gmail.com.

УДК 004.056.55

Р. С. ГАНЗЯ

ВДОСКОНАЛЕННЯ МЕТОДУ НОРМУВАННЯ В КІЛЬЦІ Р-АДИЧНИХ ЧИСЕЛ

Аналізуються методи обчислення норми елемента в кільці р-адичних чисел. Пропонується використання альтернативного методу обчислення результанта через детермінант матриці Сильвестра, що може бути застосований для розрахунку норми елемента. Наводиться наша модифікація такого метода обчислення норми через зменшену матрицю Сильвестра. В роботі показано розрахунок теоретичної складності виконання методів, а також представлено порівняння теоретичних та практичних значень обчислення норми. Результати досліджень можуть бути використані при обчислені порядку еліптичних кривих в певних системних рішеннях.

Ключові слова: порядок еліптичної кривої, обчислення норми, матриця Сильвестра, результант.

Анализируются методы вычисления нормы элемента в кольце р-адических чисел. Предлагается использование альтернативного метода вычисления результанты через детерминант матрицы Сильвестра, который может быть применен для расчета нормы элемента. Приводится наша модификация такого метода вычисления нормы через уменьшенную матрицу Сильвестра. В работе показано расчет теоретической сложности выполнения методов, а также представлено сравнение теоретических и практических значений вычисления нормы. Результаты исследований могут быть использованы при вычислении порядка эллиптических кривых в определенных системных решениях.

Ключевые слова: порядок эллиптической кривой, вычисление нормы, матрица Сильвестра, результант.

In this paper, we show the main stages of the procedure of elliptic curves order computation, which are defined over binary field. The main attention is paid to the analysis of computational complexity (time complexity) of known methods for norm computation and research the phase of normalization in the generation elliptic curves.

The paper proposes the use of an alternative method of calculation resultants through determinants Sylvester's matrix, that can be used to compute the norm of the element. However, this improvement is due to computation determinant internal structure Sylvester's matrix and basic operations. This reduces the overall complexity of the norm computation for almost 30%. We provide an assessment of theoretical complexity of this method and compare with other methods of norm computation Using practical implementation of explore methods we note the similarity of theoretical and practical evaluations of norm computation.

The research results can be used for counting order of the elliptical curves in specific system solutions. The advantage of methods based on resultants is with using other module: is the possibility of parallelizing computations of determinant (while the analytical method cannot be parallelizing) and a lot more speed in that case. In fact, our modification of the method of norm computation is optimal in terms of computational complexity for the case when you need to switch between bases for norm computation.

Keywords: order of the elliptic curve, norm computation, Sylvester's matrix, resultant.

Вступ. В Україні та в світі дуже швидко прогресують інформаційні технології. В еру активного розвитку технологій кожен день з'являються нові інформаційні сервіси та послуги, що облегшують кінцевим користувачам існування в "інформаційному світі" та додають нові можливості. При цьому питання захисту інформації стає все актуальнішим. Для забезпечення безпеки інформаційних ресурсів в каналах зв'язку в України на рівні держави прийняті стандарти, що містять криптографічні алгоритми для виконання даних задач. Такі стандарти є або власні національні (ДСТУ 4145-2002, ДСТУ 7664-2014, ДСТУ 7624-2014), або гармонізовані міжнародні (ДСТУ ISO/IEC 14888, ДСТУ ISO/IEC 9796 та інші).

При використанні алгоритмів зі стандартів, розробники систем в більшості випадкові використовують рекомендовані у стандартах значення та показники. Наприклад, для національного стандарту електронного цифрового підпису (далі – ЕЦП) визначені наступні загальносистемні параметри: поле, на якому визначена еліптична крива (далі – ЕК); коефіцієнти

рівняння кривої; порядок ЕК; базова точка ЕК; порядок базової точки; кофактор. Перелічені параметри містяться в стандарті в якості рекомендованих відповідно до рівня стійкості (максимальний розмір базової точки 431 біт. В українському стандарті ДСТУ-4145-2002 не визначена процедура генерування загальносистемних параметрів і процес формування рекомендованих параметрів зі стандарту також невідомий

Аналіз літературних даних та постановка проблеми. Відповідно до вимог з національного стандарту нами була запропонована методологія генерування загальносистемних параметрів ЕК для ДСТУ 4145-2002 [1]. Проте як показує аналіз даних у [2, 3, 4] існують об'єктивні причини збільшення розмірів загальносистемних параметрів крипто перетворень в групі точок еліптичних кривих.

Основна задача при формуванні загальносистемних параметрів для використання в групах точок ЕК зводиться до складного, з точки зору обчислення, завдання – обчислення кількості точок на ЕК [5]. Задача обчислення кількості точок на ЕК є нетривіальною і на даний момент в Україні відсутні у доступних джерелах дані про порядок виконання та сутність цього етапу. Проте в роботах [6–10] наводиться огляд і доказ математичних методів, що можуть використовуватися для обчислення кількості точок на ЕК.

Певні алгоритми та методи, що здатні обчислити порядок ЕК для бінарного поля (саме таке поле використане в ДСТУ 4145-2002) мають наступні кроки свого виконання:

1) Обчислення полінома, що задає поле (може бути переобчислений);

2) Обчислення елемента $C_j(\theta)$ для знаходження оберненої підстановки Фробеніуса (може бути переобчислений) [8];

3) Підняття *j*-інваріанту кривої до необхідної точності;

4) Знаходження значення c_0 з виразу $V_p^*(\tau) = c_0\tau_0 + O(\tau_0^2)$, більше детально цей крок для характеристики поля 2 описано у роботі Ск'єрни [10] або Веркаутерена [7];

5) Нормування коефіцієнтів значення з кроку 4 та отримання сліду ендоморфізму Фробеніуса;

6) Отримання значення порядку еліптичної кривої як $\#E(F_q) = 1 + q \pm t$, де t - значення, що отримане на попередньому кроці.

В наших попередніх роботах [2, 3] ми детально проаналізували та запропонували певні модифікації для кроків 1-4 обчислення $\#E$. Перші кроки алгоритмів обчислення порядку еліптичних кривих можуть бути обчислені з використанням *p-адичних* алгоритмів [8-10]. Оптимальним з точки зору обчислювальної складності є метод з роботи [9]. В роботі [7] наведена пропозиція щодо використання нормування для c_0 з метою отримання значення ендоморфізму Фробеніуса.

На даний момент існує аналітичний метод для обчислення норми [8] та метод на основі результанта [9]. Загальні відомості про обчислення норми описані авторами у [11]. Більш детально особливості даних методів, а також їх обчислювальні та просторові складності, будуть проаналізовані далі в роботі.

При цьому математика в кільці *p-адичних* чисел, що необхідна побудови програмної моделі, описана в роботах [12, 13]. В якості основного критерію при дослідження будемо використовувати критерій часової складності (швидкодії) обчислення норми елемента в кільці та гарантії властивостей відповідних загальносистемних параметрів.

Ціль та задачі дослідження. Метою досліджень є визначення оптимального за часовим показником алгоритму нормування, що може бути використаний при побудові загальних параметрів еліпсисних кривих.

Для досягнення поставленої мети були поставлені наступні завдання:

1. Аналіз та порівняння методів нормування, що можуть бути використанні для *p-адичних* алгоритмів.

2. Модифікація одного з методів, що може бути використаний в певних системних рішеннях при генерації власних (нерекомендованих у стандарті) загальних параметрів для ЕК, що визначена над двійковим полем.

3. Оцінка схожості теоретичної складності з практичною складністю порівнюваних алгоритмів.

Матеріали та методи дослідження методів нормування. Останнім важким з точки зору обчислювальної складності кроком при обчисленні порядку еліптичної кривої є процес обчислення норми. В загальному випадку можна представити дану задачу наступним чином: необхідно обчислити

$$\mathrm{N}_{Q_p/Q_p}(\alpha) = \prod_{i=0}^{n-1} \Sigma^i(\alpha), \qquad (1)$$

де $\alpha \in Z_q$.

Під виразом $\Sigma^i(\alpha)$ слід розуміти процес обчислення підстановки Фробеніуса, детально опис цього виразу можна знайти у [13].

Одним з перших алгоритмів обчислення норми був алгоритм Кедля [14], який запропонував використання звичайного піднесення в квадрат та множення, шляхом обчислення:

$$\alpha_{i+1} = \Sigma^{2i}(\alpha_i) * \alpha_i, \qquad (2)$$

для $\mathrm{i} = 0,...,\lfloor \log_2 n \rfloor$ з $\alpha_0 = \alpha$. Так комбінуючи це вираз можна відновити $\mathrm{N}_{Q_p/Q_p}(\alpha) = \Sigma^{\mathrm{n}-1}(\alpha)...\Sigma(\alpha)\alpha$.

Нехай $\mathrm{n} = \sum_{\mathrm{i}=0}^{l} n_i 2^i$ з $n_i \in \{0,1\}$ та $n_l = l$, тоді можемо записати наступним чином:

$$\mathrm{N}_{Q_p/Q_p}(\alpha) = \prod_{i=0}^{l} \Sigma^{2^{i+1}+2^{i+2}+...+2^l}(\alpha_i^{n_i}), \qquad (3)$$

де сума $2^{i+1} + 2^{i+2} + ... + 2^l$ визначається нулем для $i \geq l$.

Даний алгоритм є особливо привабливим для *p-адичних* полей з Гаусовим нормальним базисом малих характеристик, тому що там можливе ефективне і швидке обчислення підстановки Фробеніуса [8]. І в

такому випадку складність обрахування складає $O(\log n)$ множень та стільки ж обчислень підстановки Фробеніуса в $Z_q/(p^N Z_q)$, що складає приблизно $O((nN)^\mu \log n)$ бітових операцій з просторовою складністю $O(nN))$. Для інших базисів даний алгоритм практично не використовується через доволі велику складність обчислення підстановки Фробеніуса.

Множення двох цілих чисел, що складаються з n біт, здійснено за $O(n^\mu)$ операцій, де μ – це константа, яка визначає час виконання множення двох m бітових цілих чисел з часовою складністю $O(m^\mu)$. Так для класичних алгоритмів множення значення $\mu = 2$ для швидкого алгоритму Карацуби, слідуючи роботі [9], $\mu = \log_2 3$.

Проте для практичного використання більш цікавим є аналітичний метод обчислення норми, що був запропонований у роботі [8]. Автори методу канонічного підйому Сато-Ск'єрна-Тагучі еліптичної кривої також запропонували і метод нормування. Нехай $\exp(x) = \sum_{i=0}^{\infty} x^i / i!$ та $\log(x) = \sum_{i=1}^{\infty} (-1)^{i-1}(x-1)^i / i$ будуть *p-адичними* функціями експоненти та логарифму (у загальному випадку). Легкі обчислення показують нам, що $\exp(x)$ сходиться для $\mathrm{ord}_p(x) > 1/(p-1)$ та $\log(x)$ сходиться для $\mathrm{ord}_p(x-1) > 0$.

Припустимо спочатку, що α є близьким до одиниці, тобто $\mathrm{ord}_p(\alpha - 1) > 1/(\mathrm{p}\text{-}1)$, тоді:

$$\mathrm{N}_{Q_p/Q_p}(\alpha) = \exp(\mathrm{Tr}_{Q_p/Q_p}(\log(\alpha))), \qquad (4)$$

оскільки Σ є безперервним, то обидва ряди сходяться. Головним кроком в даному алгоритмі (4) є оцінка функції логарифма. Використовуючи загальний випадок обчислення функції логарифма ("сирий метод") на це буде необхідно $O(\mathrm{N})$ множень в $Z_q/(p^N Z_q)$ або $O(n^\mu N^{\mu+1})$ бітових операцій.

Автори ж роботи [8] запропонували інше вирішення цієї проблеми. Зокрема вони зазначили, що значення α^{p^k} для $k \in N$ є дуже близьким до одиниці, тобто $\mathrm{ord}_p(\alpha^{p^k} - 1) > k + \frac{1}{p-1}$. Якщо $\alpha \in Z_q/(p^N Z_q)$, тоді α^{p^k} визначається і в $Z_q/(p^{N+k} Z_q)$ та може бути обчислено за $O(k)$ множень в $Z_q/(p^{N+k} Z_q)$. В подальшому зауважимо, що

$$\log(\alpha) \equiv p^{-k}(\log(\alpha^{p^k})(\mathrm{mod}\ p^{N+k}))(\mathrm{mod}\ p^N). \qquad (5)$$

В такому випадку логарифм, що обчислюється всередині виразу (5) може бути обчислений з використанням $O(N/k)$ операція множення над $Z_q/(p^{N+k} Z_q)$. Тому якщо взяти $k \approx \sqrt{N}$, тоді обчислити значення логарифму (всього виразу з 5) можна за $O(n^\mu N^{\mu+0,5})$ бітових операцій.

Для двійкових полів автори у [8] пропонують додаткове вдосконалення і на цей раз воно стосується напряму функції обчислення логарифму. Так як $\mathrm{ord}_p(\alpha - 1) > 1$, ми маємо $\alpha \equiv 1 (\mathrm{mod}\ 2^v)$ для $v \geq 2$. Нехай $z = \alpha - 1 \in 2^v Z_q/(2^N Z_q)$ і тоді визначимо

$$\gamma = \frac{z}{2+z} \in 2^{v-1} Z_q/(2^{N-1} Z_q). \qquad (6)$$

Тоді $\alpha = \frac{1+\gamma}{1-\gamma}$ і тому:

$$\log(\alpha) \equiv \log(1+z) = 2\sum_{j=1}^{\infty} \frac{\gamma^{2j-1}}{2j-1}. \qquad (7)$$

Зауважимо, що всі знаменники у виразі (7) є непарними. Приведення цього рівняння за модулем 2^N привиде до наступного

$$\log(\alpha) \equiv \log(1+z) = 2 \sum_{1 \leq (v-1)(2j-1) < m-1}^{\infty} \frac{\gamma^{2j-1}}{2j-1} (\mathrm{mod}\ 2^N). \qquad (8)$$

Наступним кроком при обчислені норми за аналітичним методом (4) є крок обчислення сліду Tr_{Q_p/Q_p}. Дана задача представляються наступним чином: визначаємо $\alpha_i \in Z_p$, *як* $\log(\alpha) \equiv \sum_{i=0}^{n-1} \alpha_i t^i (\mathrm{mod}\ p^N)$ і тоді

$$\mathrm{Tr}_{Q_p/Q_p} \log(\alpha) \equiv \sum_{i=0}^{n-1} \alpha_i \mathrm{Tr}_{Q_p/Q_p}(t^i) (\mathrm{mod}\ p^N), \qquad (9)$$

в даному виразі кожен $\mathrm{Tr}_{Q_p/Q_p}(t^i)$ для $i = 0,...,n-1$ може бути передобчислений з використанням формули Ньютона:

$$\mathrm{Tr}_{Q_p/Q_p}(t^i) + \sum_{j=1}^{i-1} \mathrm{Tr}_{Q_p/Q_p}(t^{i-j}) * f_{n-j} + i * f_{n-i} \equiv 0 (\mathrm{mod}\ p^N). \qquad (10)$$

В наведеному вище виразу під $f(t) = \sum_{i=0}^{n} f_i t^i$ мається на увазі поліном, що задає розширення кільця *p-адичних* чисел $Q_q \cong Q_p[t]/(f(t))$.

Нехай $t_a = Tr_{Q_p/Q_p}(\log(a)) \in Z_p$ тоді $ord_p(t_a) > 1/(p-1)$, отже $t_a \in pZ_p$ для $p \geq 3$ та $t_a \in 4Z_2$ для $p = 2$. Якщо передобчислити $\exp(p) (\mathrm{mod}\ p^m)$ для $p \geq 3$ або $\exp(4) (\mathrm{mod}\ p^m)$ для $p = 2$, отримаємо:

$$\exp(t_a) \equiv \exp(p)^{t_a/p} (\mathrm{mod}\ p^m) \quad для \quad p \geq 3, \qquad (11)$$

$$\exp(t_a) \equiv \exp(4)^{t_a/p} (\mathrm{mod}\ 2^m) \quad для \quad p = 2, \qquad (12)$$

після чого використовуючи звичайні алгоритми піднесення в квадрат та множення обчислимо $\exp(t_a)$. Тому, якщо значення α близьке до одиниці обчислення норми за алгоритмом (4) може бути обраховане з використанням $O(n^{\mu}N^{\mu+0,5})$ бітових операцій та з просторовою складністю $O(nN)$.

Зауважимо, що для $p=2$ ми припускаємо, що $ord_p(\alpha-1)>1/(p-1)$; тоді як для $p\geq 3$ необхідно розглядати більш загальну ситуацію, де $\alpha\in Z_q$ не наближається до одиниці. Нехай $\bar{\alpha}\in F_q$ означає залишок по модулю p, а $\alpha_t\in Z_q$ значення підняття Тейхмюллера, тобто унікальний $(q-1)$-ий корінь одиниці, який зводиться до $\bar{\alpha}$. Розглянемо рівність

$$\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha)=\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha_t)\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha_t^{-1}\alpha); \qquad (13)$$

тоді $ord_p(\alpha_t^{-1}\alpha-1)\geq 1>1/(p-1)$, так як p непарне. Крім того, зауважимо, що $\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha_t)$ дорівнює підняттю Тейхмюллера $\mathrm{N}_{\mathrm{F_p}/F_p}(\bar{\alpha})$. Головна проблема в даному випадку обчислення підняття Тейхмюллера елемента. Використовуючи метод ітерацій Ньютона для $X^{1-q}-1=0$, $\alpha(\mathrm{mod}\,p^N)$ може бути обчислений з використанням $O(n^{2\mu+1})$ бітових операцій та з просторовою складністю $O(n^2)$. Сато у роботі [12] вказав, що підняття Тейхмюллера α_t може бути ефективно обчислене як рішення

$$\sum(\mathrm{X})=\mathrm{X}^{\mathrm{p}} \quad ma \quad \mathrm{X}\equiv\bar{\alpha}(\mathrm{mod}\,p). \qquad (14)$$

Опираючись на метод SST [ ] можна стверджувати, що α_t може бути обчислений з

$$\sum{}^{-1}(\mathrm{X}^{\mathrm{p}})=\mathrm{X} \quad ma \quad \mathrm{X}\equiv\bar{\alpha}(\mathrm{mod}\,p), \qquad (15)$$

і використовуючи той самий трюк, що використаний в методі SST отримаємо, що для $W\approx n^{\mu/(1+\mu)}$ та $N\approx n/2$ складність такого обчислення складає $O(n^{2\mu+1/(1+\mu)})$ бітових операцій (не враховуючи складність передобчислень) та просторова складністю $O(n^2)$.

Третій тип обчислення норми був запропонований Харлі у тій же роботі [9], де і метод підняття еліптичних кривих. Харлі запропонував асимптотично швидкий алгоритм обчислення норми, що базується на класичній формулі з теорії чисел, що представляє норму як результант. Сам результант може бути обчислено за допомогою адаптивного швидкого розширеного алгоритму пошуку НСД Моенка [15].

Нехай $Z_q=Z_p[\theta]$ з θ, який є коренем незвідного многочлена $f(x)\in Z_p[x]$ степені n. Тоді $f(x)$ повністю розщеплюється через Z_q як $f(x)=\prod_{\mathrm{i}=0}^{\mathrm{n-1}}(\mathrm{x}-\sum^{\mathrm{i}}(\theta))$, де $\sum^{\mathrm{i}}$ є підстановкою Фробеніуса відповідної степені.

Так для $\alpha\in \mathrm{Q_q}$ отримаємо

$$\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha)=\mathrm{p}^{\mathrm{n}\,\mathrm{ord_p}(\alpha)}\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha/p^{\mathrm{ord_p}(\alpha)}).$$

Нехай $\alpha=\sum_{\mathrm{i}=0}^{\mathrm{n-1}}a_i\theta^i$ буде одиницею в Z_q і визначимо $A(x)=\sum_{\mathrm{i}=0}^{\mathrm{n-1}}a_ix^i\in Z_p[x]$. За визначенням норми та результанта отримаємо наступне

$$\mathrm{N}_{\mathrm{Q_p}/Q_p}(\alpha)=\prod_{\mathrm{i}=0}^{\mathrm{n-1}}(\sum^{\mathrm{i}}(\alpha))=\prod_{\mathrm{i}=0}^{\mathrm{n-1}}\mathrm{A}(\sum^{\mathrm{i}}(\theta))= \qquad (16)$$
$$=\mathrm{Re}\,s(f(x),A(x)).$$

Так результант $\mathrm{Re}\,s(f(x),A(x))$ може бути обчислений майже в лінійний час, використовуючи варіант швидкого розширеного алгоритму пошуку НСД Моенка. Детально даний алгоритм описаний в [7], в даній роботі будуть наведені короткі відомості для побудови алгоритму нормування. Головна ідея алгоритму Моенка полягає у тому, що перша частка в алгоритмі Евкліда залежить тільки від найвищих коефіцієнтів вхідних поліномів.

Нехай $f=f_{\mathrm{n}}x^{\mathrm{n}}+\ldots+f_0\in K[x]$ буде поліном степені n над полем K і $f_{\mathrm{n}}\neq 0$. Усічений поліном $f\,|\,k$ визначається як

$$f|\mathrm{k}=f_{\mathrm{n}}x^{\mathrm{k}}+\ldots+f_{n-k}, \qquad (17)$$

де $f_{\mathrm{i}}=0$ для $\mathrm{i}<0$. Крім того, дві пари поліномів (f,g) та (f^*,g^*) збігаються з точністю до k, якщо

$$f\,|\,k=f^*\,|\,k,$$

$$g\,|(k-(\deg f-\deg g))= \qquad (18)$$
$$=g^*\,|(k-(\deg f^*-\deg g^*)).$$

Враховуючи пару поліномів $\mathrm{r_0}$ та $\mathrm{r_1}$ з $\deg \mathrm{r_0}>\deg r_1$, алгоритм Евкліда обчислює наступний вираз

$$r_{i-1}=q_ir_i+p_{i+1}r_{i+1}, \qquad (19)$$

з $q_i,r_i\in K[x]$, $p_{i+1}\in K$ для $i=0,\ldots,l$, $r_{l-1}=q_lr_l$. Нехай $m_i=\deg q_i$ для , $k\in N$ визначимо значення $\eta(k)\in N$ наступним чином

$$\eta(k)=\max\{0\leq j\leq l\,|\,\sum_{1\leq i\leq j}m_i\leq k\}. \qquad (20)$$

Базисом для алгоритму Моенка є лема, яка стверджує, що частки в алгоритмі Евкліда залежать тільки від самого високого значення коефіцієнтів на вході. Доведення даної леми наведено у [15]. Лема полягає у наступному, нехай $k\in N$ і припустимо, що (f,g) та (f^*,g^*) збігаються з точністю до $2k$, тоді

$\eta(k) = \eta^*(k), q_i = q_i^*$ та $p_{i+1} = p_{i+1}^*$ для $1 \le i \le \eta(k)$, з частками q_i, q_i^* та з старшими коефіцієнтами залишків p_{i+1}, p_{i+1}^*, що обчислені з використанням алгоритму Евкліда на вході з (f,g) та (f^*,g^*) відповідно.

Дана лема дозволяє зробити рекурсивний алгоритм обчислення розширеного алгоритму пошуку НСД двох поліномів. Так, для обчислення результанта необхідно стежити за скалярами $p_i \in K$ для $i = 0,...,l$. Дана лема сформульована так: нехай $f,g \in K[x]$ та мають степені $n = n_0$ та $n_1 \le n_0$ відповідно. Нехай $n_2,...,n_l$ будуть степенями залишків в алгоритмі Евкліда для (f,g), а $p_0,...,p_l$ їх найбільш значущі коефіцієнти. Якщо $\gcd(f,g) = 1$, тоді

$$\mathrm{Res}(f,g) = (-1)^{\tau} p_0^{l} \prod_{1 \le j \le l} p_j^{n_{j-1}}, \qquad (21)$$

з $\tau = \sum_{1 \le j \le l} n_{j-1} n_j$. Результант за такою формулою може бути обчислений використовуючи $O(n^{\mu} \log n)$ бітових операцій.

Хоча алгоритм 4 має квадратичну часову складність свого виконання, він не є особливо привабливим для застосування у криптографічних додатках. Щоб відновити правильну норму по модулю p^N її треба обчисляти за модулю p^{Nc} з малою константою c, що залежить від мінімального значення коефіцієнтів β / a_d, тому на практиці краще використовувати нормування за алгоритмом 3. Мінімальна обчислювальна складність такого методу виходить $O((nN)^{\mu} \log n)$.

Інша пропозиція методу обчислення норми через результант. З формули (16) видно, що для обчислення норми можна використати результант і Харлі запропонував метод, що має квадратичну складність свого виконання, проте на практиці її використовувати немає сенсу і краще використати аналітичний алгоритм обчислення норми, показаний у [8].

Пропозиція 1. Для обчислення результанта можна використати одну з його властивостей, а саме те, що результант дорівнює значенню матриці Сильвестра [16].

Добре відомо, що алгоритм Евкліда для обчислення найбільшого спільного дільника (НСД) двох цілих чисел відомий понад дві тисячі років, і, як з'ясовується, це найстаріший з відомих алгоритмів. Інтерес до обчислення НСД двох многочленів вперше з'явився тільки в шістнадцятому столітті, і проблема були вирішена Саймоном Стевіні [16]. Суть ідеї проста – просто застосувати алгоритм Евкліда (для цілих чисел) тільки до многочленів з цілими коефіцієнтами. Однак, з обчислювальної точки зору, застосування алгоритму Евкліда до многочленів з цілими коефіцієнтами є дуже неефективним через зростання самих значень коефіцієнтів, що врешті-решт уповільнює обчислення. Таке зростання коефіцієнтів пов'язане з тим, що кільце $Z[x]$ не є евклідовим, і, отже, ділення (як ми його знаємо) не завжди може бути виконане.

Таким чином, проблема такого підходу полягає в тому, що коефіцієнти многочленів зростають в геометричній прогресії, і, отже, уповільнюють обчислення. Для контролю росту коефіцієнтів і позбавлення необхідності кожен раз обчислювати НСД коефіцієнтів Сильвестр у своїй статті в 1853 році запропонував інший підхід (а у 1948 Хабіхт довів ідею до кінця).

Ідея полягає у вирішені описаної вище проблеми за допомогою триангуляції матриці, така форма матриці в даному випадку називається матриця Сильвестра, що дозволяє уникнути явного ділення поліномів. Так Сильвестр запропонував один із методів уникнення росту коефіцієнтів [16].

Побудова матриці Сильвестра здійснюється наступним чином, припустимо маємо два поліноми в $Z[x]$, $p_1(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_0$ та $p_2(x) = b_m x^m + b_{m-1} x^{m-1} + ... + b_0$, причому коефіцієнти $a_n \ne 0$, $b_m \ne 0$ та $n > m$. Взагалі існує декілька форм представлення матриці (форма ді Бруно та форма Труді), зупинимось на формі ді Бруно. Отже результант двох поліномів $p_1(x)$ та $p_2(x)$ при обчислені з використанням матриці Сильвестра виглядає наступним чином:

$$\mathrm{res}(p_1(x), p_2(x)) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_0 & & \dots & 0 \\ & & & & & \vdots & & \\ 0 & 0 & \dots & & a_n & a_{n-1} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_0 & 0 & \dots & 0 \\ & & & & \vdots & & & \\ 0 & 0 & \dots & b_m & b_{m-1} & & \dots & b_0 \end{vmatrix}. \qquad (22)$$

Матриця Сильвестра має $n+m$ рядків та $n+m$ стовпчиків, для отримання значення результанта необхідно обчислити детермінант даної матриці. Обчислення детермінанта можна виконати будь-яким відомим способом для цілих чисел, проте є певні особливості, пов'язані з операціями в кільці *p-адичних* чисел а саме: обчислення виконуються в кільці, тому операцію ділення треба замінити на множення оберненого елемента, всі операції необхідно виконувати за модулем заданої точності *N*.

Для прикладу далі сформуємо наступну задачу, нехай маємо кільце *p-адичних* чисел Z_{2^7}, що визначається як $Z_2[X] / M(x)$ з $M(x) = x^7 + x + 1$ (зауважимо, що в даному випадку використовуємо модуль у розрядженій формі, а не у формі Тейхмюллера), елемент з кільці $a(x) = 40x^6 + 32x^5 + 44x^4 + 4x^2 + 60x + 53$, а точність $N = 6$. Необхідно розрахувати норму даного елемента або відповідно до (16) результант поліномів $M(x)$ та $a(x)$. Для цього сформуємо матрицю Сильвестра, що виглядає наступним чином:

$$M_s = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 \end{vmatrix}. \quad (23)$$

Детермінант даної матриці був обчислений з використанням метода Гауса і тоді маємо наступний вираз:

$$\det(M_s) = 484537365 (\bmod 2^6) = \\ = 21 = \mathrm{Res}(M(x), a(x) = N_{Q_p/Q_p}(a)) . \quad (24)$$

Далі розглянемо детально метод обчислення детермінанта та нашу модифікацію для його подальшого використання при обчислені порядку еліптичних кривих.

Модифікація методу обчислення норми через результант. Аналізуючи матрицю з (23), а також модулі, що будуть використовуватись при обчислені порядку еліптичних кривих, можна зробити висновок, що матриця Сильвестра завжди буде мати схожий на (23) вигляд. Мається на увазі, що коефіцієнт матриці $a_{0,0}$ буде завжди дорівнювати одиниці і він завжди буде зміщатися на один вниз та на один вправо і переходити в $a_{1,1}$ і далі в наступний елемент головної діагоналі аж до $a_{n=2,n-2}$, після цього за схожим принципом буде розміщено елемент щодо якого необхідно розрахувати норму.

Пропозиція 2. Для обчислення детермінанта матриці Сильвестра оптимальним є використання метода Гауса.

Аналіз матриці (22) та (23), як прикладу, показує, що в матриці дуже багато нульових елементів у верхній частині матриці, а елементи головної діагоналі від $a_{0,0}$ до $a_{n=2,n-2}$ дорівнюють одиниці. З використанням такої особливості метод Гауса є дуже привабливим з точки зору оптимізації обчислень при нормуванні.

Суть методу Гауса полягає у приведені матриці до трикутного виду (виконання тріангуляції матриці) шляхом еквівалентних перетворень. До таких перетворень відносяться:

- перестановка рядків;
- додавання до елементів одного рядка відповідних елементів іншого рядка, множення на константу.

Виконання над матрицею еквівалентних перетворень не змінить значення детермінанта матриці заданої матрицею. Побудова трикутної матриці є частиною алгоритму Гаусса-Жордана рішення СЛАР, а також обчислення детермінанта методом Гауса.

Для «обнулення» елементів *і-того* стовпця матриці досить до всіх рядків з номерами $j = i+1,...,n$ (n – розмір матриці) додати *і-ий* рядок, помножений на $-a_{j,j} / a_{i,i}$ (варто зауважити, що всі операції повинні виконуватись в кільці *р-адичних* чисел, зокрема операція ділення повинна бути замінена на множення і пошук оберненого елмента). При виконанні такої операції може виникати потреба ділення на нуль, якщо елемент на головній діагоналі виявиться рівним нулю - в цьому випадку виконують перестановку рядків матриці. Найбільш ефективним підходом до перестановки рядків є перестановка *і-того* рядка з рядком, що має максимальний по модулю елемент в *і-тому* стовпці. Доведено, що при виконанні такої перестановки для кожного рядка (а не тільки коли $a_{i,i} \equiv 0$) для матриці з ненульовим детермінантом ми завжди знайдемо рядок для заміни.

В нашому випадку (23) ми можемо множити елемент головної діагоналі на елементи, що знаходяться під ним і поступово "обнулити" майже половину матриці, а враховуючи те, що на головній діагоналі завжди знаходяться одиниці в даному випадку не потрібно навіть знаходити обернений елемент до нього, після проходу елементів головної діагоналі до $a_{n=2,n-2}$ (n – розмір базового поля) з використанням елементарних перетворень матриця M_s прийме наступний вигляд:

$$M_s = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 13 & 56 & 52 & 20 & 60 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 60 & 13 & 56 & 52 & 20 & 60 & 60 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 60 & 13 & 56 & 52 & 20 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4 & 60 & 13 & 56 & 52 & 20 \\ 0 & 0 & 0 & 0 & 0 & 0 & 44 & 0 & 4 & 60 & 13 & 56 & 32 \\ 0 & 0 & 0 & 0 & 0 & 0 & 32 & 44 & 0 & 4 & 60 & 13 & 24 \\ 0 & 0 & 0 & 0 & 0 & 0 & 40 & 32 & 44 & 0 & 4 & 60 & 53 \end{vmatrix}. \quad (25)$$

Для проведення такої модифікації на необхідно виконати

Пропозиція 3. Обчислення детермінанта матриці Сильвестра можна умовно розділити на 2 етапи: перший етап – "обнулення" половини матриці з використанням особливостей її побудови і метода тріангуляції матриці; другий етап – обчислення детермінанта зменшеної матриці, що починається з елемента головної діагоналі $a_{n=1,n-1}$.

Аналізуючи для прикладу матрицю M_s, що відображена у (25), можна зробити висновок, що при знаходженні добутку елементів головної діагоналі (заключний етап метода Гауса) для визначення детермінанта, значення завжди будуть мати лише елементи нижче *n-1* рядка, бо інші будуть дорівнювати одиниці, що не змінить значення детермінанта. Враховуючи

таку отриману особливість, можна зробити висновок, що так як значення елементів, що знаходяться вище *n-1* рядка і лівіше від *n-1* стовпчика (так як вони вже дорівнюють нулю) не здійснюють впливу на обчислення детермінанта матриці, ми можемо перейти до зменшеної матриці, що формується з *n-1* рядка та *n-1* стовпчика, і провести її обчислення будь-яким іншим зручним способом (не обов'язково метод Гауса). Зменшена матриця M_{sn} (розмірність такої матриці буде *n*x*n*) відображена нижче:

$$M_{sn} = \begin{vmatrix} 13 & 56 & 52 & 20 & 60 & 0 & 4 \\ 60 & 13 & 56 & 52 & 20 & 60 & 60 \\ 4 & 60 & 13 & 56 & 52 & 20 & 0 \\ 0 & 4 & 60 & 13 & 56 & 52 & 20 \\ 44 & 0 & 4 & 60 & 13 & 56 & 32 \\ 32 & 44 & 0 & 4 & 60 & 13 & 24 \\ 40 & 32 & 44 & 0 & 4 & 60 & 53 \end{vmatrix}. \quad (26)$$

Для обчислення детермінанта M_{sn} можна використати будь-який відомий метод. Так, метод обчислення за мінорами має складність $O(2^n n)$, метод Гауса має складність $O(n^3)$. Одним з найкращих є метод декомпозицій (існують методи декомпозицій LU, QR та інші), такі методи мають таку ж складність як і метод Гауса [17]. Але якщо дві матриці порядку *n* можуть бути помножені за час $M(n)$, де $M(n) \geq n^a$, для деякого $a > 2$, то детермінант може бути обчислений зі складністю $O(M(n))$ [18]. Це означає, що, наприклад, при використані для множення алгоритм Копперсміат-Винограда, складність обчислення детермінанта буде складати $O(n^{2,376})$.

Наприклад, продовження використання метода Гауса і приведення матриці до трикутного виду перетворить зменшену матрицю M_{sn} у наступну

$$M_{sn} = \begin{vmatrix} 13 & 56 & 52 & 20 & 60 & 0 & 4 \\ 0 & 45 & 8 & 4 & 4 & 60 & 12 \\ 0 & 0 & 29 & 56 & 20 & 4 & 32 \\ 0 & 0 & 0 & 13 & 56 & 20 & 36 \\ 0 & 0 & 0 & 0 & 13 & 56 & 48 \\ 0 & 0 & 0 & 0 & 0 & 13 & 56 \\ 0 & 0 & 0 & 0 & 0 & 0 & 53 \end{vmatrix}. \quad (27)$$

Добуток елементів головної діагоналі в даному випадку і дасть нам такий самий результат як і в (24).

Результати дослідження обчислювальної складності і програмна реалізація методів нормування

Відразу зауважимо, що складність арифметичних операцій в $Z_p / p^N Z_p = Z / p^N Z$ наведена у табл. 1.

Складність арифметичних операцій в $Z_q / p^N Z_q = Z[x] / (p^N, f(x))$, де $f \in \mathrm{Z[x]}$ і є незвідним многочленом за модулем *p* наведена у табл. 2.

Таблиця 1 – Складність операцій в кільці p-адичних чисел

№	Операція	Часова складність	Просторова складність
1	Додавання	$O(\log_2(p^N))$	$O(\log_2(p^N))$
2	Віднімання	$O(\log_2(p^N))$	$O(\log_2(p^N))$
3	Множення	$O((\log_2(p^N))^\mu)$	$O((\log_2(p^N))^2)$
4	Пошук експоненти	$O((\log_2(p^N))^{\mu+1})$	$O((\log_2(p^N))^2)$
5	Інверсія	$O((\log_2^2(p^N))^\mu)$	$O((\log_2^2(p^N))^\mu)$

Таблиця 2 – Складність операцій в розширені кільці p-адичних чисел

№	Операція	Часова складність	Просторова складність
1	Додавання	$O(\log_2(p^n))$	$O(\log_2(p^n))$
2	Віднімання	$O(\log_2(p^n))$	$O(\log_2(p^n))$
3	Множення	$O((N^\mu \log_2(p^n))^\mu)$	$O((N^2 \log_2(p^n))^2)$
4	Пошук експоненти	$O((N^{\mu+1} \log_2(p^n))^{\mu+1})$	$O((N^2 \log_2(p^n))^2)$
5	Інверсія	$O((N^\mu \log_2(p^n))^\mu)$	$O((N^2 \log_2(p^n))^2)$

Дані про складність виконання обчислень взяті з [19] та адаптовані з використанням інформації про *p-адичні* операції з [13]. Надалі будемо розраховувати теоретичну складність обчислень з урахуванням того, що $p = 2$, тобто проведемо адаптацію під національний стандарт ДСТУ 4145-2002.

Детальний опис і аналіз алгоритмів нормування проведено в попередніх розділах. Далі зупинимося на нашій модифікації алгоритму обчислення норми через результант з використанням матриці Сильвестра. Складність обчислення детермінанту з використанням методу Гауса складає $O(n^3)$ операцій, враховуючи складність операцій в кільці $Z / p^N Z$, результуюча складність метода Гауса для проведення етапу нормування складає, за нашими грубими оцінками, прибли-

зно $O(n^3(N)^\mu)$. Порівнювати складність обчислювання результанта будемо з алгоритмом нормування, визначеному у тій же роботі, де і алгоритм SST, його складність - $O(n^\mu N^{\mu+0,5})$. Далі порівняно з цим виведемо теоретичну часову складність нашої модифікації алгоритму обчислення норми через матрицю Сильвестра (відповідно до пропозиції 3).

На першому етапі алгоритму треба виконати множення одиниць у верхній частині матриці на значення елементів матриці, що знаходиться у нижній частині. Для цього необхідно виконати $i=\sum_{i=1}^{d-1} i$ множень в кільці. Так як елементи верхньої частини матриці у більшості рядка дорівнюють одиниці або нулю, то там множення робити не треба, а лише поступово замінити на необхідні значення нижньої частини матриці (мається на увазі для рядків від *n-1* до *2n-2*). Після цього необхідно поступово знайти різницю між рядками $i=0,...,d-2$ та рядками $i=n-1,...,2n-2$. Для цього необхідно здійснити операцію віднімання *2n-1* разів, потім $2(2n-2)$ разів і так далі. Таким чином складність першого етапу можна оцінити у $O\left(\left(\sum_{i=1}^{d-1} i(2n-i)\right)N\right)$ бітових операції. Якщо спростити даний вираз, то можна сказати, що необхідно приблизно $O\left(\frac{n^3}{2}N\right)$ бітових операцій.

На наступному етапі необхідно обчислити детермінант зменшеної матриці відповідно до пояснень у пропозиції 3. Далі буде наведена детальна оцінка обчислювальної складності для метода Гауса для другого етапу виконання нашої модифікації алгоритму нормування. Для виконання метода Гауса на кожній ітерації з можливих *n-1* необхідно знайти один раз обернений елемент до елемента на головній діагоналі (виконати інверсію). Після цього необхідно буде виконати $(n-i)(n-i+1)$, де $i=0,...,n-1$, операцій множення та віднімання. З кожною ітерацію (мається на увазі з переходом на інший елемент головної діагоналі, що буде "занулювати" стовпчик під ним) кількість операцій множення та віднімання різко зменшується, тому що для стовпчиків, що будуть знаходитися зліва дані операції вже роботи непотрібно. Таким чином отримаємо наступну кількість операцій:

- інверсії: *n-1*;
- множення: $\sum_{i=1}^{d-1}(n-i)(n-i+1)$;
- віднімання: $\sum_{i=1}^{d-1}(n-i)(n-i+1)$.

Якщо спростити отримані вирази для операцій множення та віднімання, то їх кількість буде дорівнювати $\frac{n^3-n}{3}$.

Після цих перетворень також додатково необхідно провести *n-1* операцій множення (елементів головної діагоналі) для визначення детермінанта зменшеної матриці. Враховуючи те, що кількість операцій інверсії та множення елементів головної діагоналі дуже незначна, порівняно з кількістю інших операцій, то ними можна знехтувати у загальній оцінці складності. Таким чином асимптотична складність метода обчислення детермінанта для зменшеної матриці складає $O\left(\frac{n^3-n}{3}N+\frac{n^3-n}{3}N^\mu\right)$ бітових операцій. Варто зауважити, що таку оцінку метода Гауса можна використати і при обчислені детермінанта матриці Сильвестра (немодифікованого методу), але за умови, що вона більша $n\to 2n-1$.

Якщо підсумувати складність модифікованого методу, то отримаємо наступний результат $O\left(\frac{n^3}{2}N+\frac{n^3-n}{3}N+\frac{n^3-n}{3}N^\mu\right)$, де μ – це константа, яка визначає час виконання множення двох m бітових цілих чисел з часовою складністю $O(m^\mu)$. Так для класичних алгоритмів множення значення $\mu=2$ для швидкого алгоритму Карацуби, слідуючи роботі [19], $\mu=\log_2 3$ (приблизно $\mu=1,6$), значення $N\approx n/2$.

Результати порівняння теоретичної обчислювальної складності алгоритмів нормування для різних розмірів базового поля наведені у табл. 3 (всі наведені результати вимірюються в бітових операціях).

Таблиця 3 – Теоретична складність оцінюваних методів нормування

Степінь розширення поля, *біт*	Алгоритм нормування, обчислювальна складність (бітових операцій)			
	Результат через швидкий алгоритм Моенка	Аналітичний метод	Результант через матрицю Сильвестра	Модифікований метод через зменшену матрицю
7	$4,7\cdot10^2$	$3,1\cdot10^2$	$9,9\cdot10^3$	$1,8\cdot10^3$
79	$2,5\cdot10^6$	$2,5\cdot10^6$	$5,2\cdot10^8$	$7,5\cdot10^7$
107	$7\cdot10^6$	$7,5\cdot10^6$	$2\cdot10^9$	$2,9\cdot10^9$
257	$1,4\cdot10^8$	$1,9\cdot10^8$	$1,1\cdot10^{11}$	$1,5\cdot10^{10}$
383	$5,2\cdot10^8$	$8,5\cdot10^8$	$7\cdot10^{11}$	$9,3\cdot10^{10}$
503	$1,3\cdot10^9$	$2,3\cdot10^9$	$2,4\cdot10^{12}$	$3,2\cdot10^{11}$
709	$4,1\cdot10^9$	$8,2\cdot10^9$	$1,2\cdot10^{13}$	$1,5\cdot10^{12}$
827	$7\cdot10^9$	$1,5\cdot10^{10}$	$2,4\cdot10^{13}$	$3,1\cdot10^{12}$
1031	$1,4\cdot10^{10}$	$3,3\cdot10^{10}$	$6,5\cdot10^{13}$	$8,5\cdot10^{12}$

За результатами оцінки табл. 3 можна зробити висновок, що оптимальним є використання алгоритму обчислення норми відповідно до швидкого знаходження НСД з використанням алгоритму Моенка, проте відповідно до зауважень [7], даний алгоритм на практиці важко реалізується і вимагає більшої кількості обчислень. Таким чином порівняно з нашими варіаціями методів обчислення норми через матрицю Сильвестра, оптимальним виходить використання аналітичного методу з [8] (запропонованого Сато, Ск'єрною та Тагучі).

Далі проведемо оцінку складності виконання даних методів з точки зору програмної реалізації. Для дослідження методів нормування, як одного кроків, обчислення кількості точок на еліптичній кривій, нами було розроблено програмний засіб на мові C++ з використанням бібліотеки NTL та gmp. Дослідження, щодо часу виконання алгоритмів проводилися на програмі, що була скомпільована з використанням gcc 4.84 на операційний системі Ubuntu 14.04 та процесорі Intrel Core i5-2300. Так як всі операції для алгоритмів виконуються послідовно, тобто розпаралелювання відсутнє, кількість ядер у складі центрального процесору неважливо.

У табл.4 наведено час обчислення норми для різних розмірів базового поля та різних методів нормування.

Таблиця 4 – Практична складність оцінюваних методів нормування

Степінь розширення поля *d*, *біт*	Алгоритм нормування		
	SST метод, *с*	Результант через матрицю Сильвестра, *с*	Модифікований метод через зменшену матрицю, *с*
7	$2{,}9\cdot10^{-4}$	$4{,}2\cdot10^{-5}$	$2{,}7\cdot10^{-5}$
79	$7{,}3\cdot10^{-3}$	$2\cdot10^{-2}$	$2\cdot10^{-2}$
107	$1\cdot10^{-2}$	$5\cdot10^{-2}$	$5\cdot10^{-2}$
257	0,05	0,9	0,7
383	0,13	3	2,7
503	0,2	7,2	6,2
709	0,5	26,1	20,1
827	0,7	53,1	41,5
1031	1,7	122,6	101

За результатами аналізу Таблиці 4 можна стверджувати, що практична обчислювальна складність модифікованого методу менша приблизно на 20 %, порівняно зі звичайним методом обчислення детермінанту матриці Сильвестра. Якщо порівнювати методи знаходження норми через результант, то вони гірші від аналітичного методу для 257 біт майже у 20 разів, для 503 у 30 разів і чим далі тим вони стають менш ефективними.

Якщо порівняти Таблицю 3 та Таблицю 4, то можна стверджувати, що практичні та теоретичні складності даних методів майже сходяться. Звичайно це зумовлено тим, що оцінка аналітичного методу є доволі грубою і теоретична оцінка не враховує інші складності, що містяться в програмних реалізаціях. Проте характер росту складності даних методів від розміру розширення базового поля спостерігається і сходиться.

Перевагою методів на основі результант є можливість розпаралелювання обчислень детермінанта, в той час як аналітичний метод розпаралелити неможливо. На даний момент ми не проводили модифікацію методів на основі обчислення детермінанта у напрямку розпаралелювання обчислень.

Обговорення результатів дослідження та проблематики використання аналітичного методу і методів на основі результанта. Автори національного стандарту електронного цифрового підпису ДСТУ 4145-2002 пропонують використовувати представлення, коли в якості модуля використовується $f(x)\in Z_q[x]$. Мається на увазі, що такий поліном є розрядженим, незвідним у $F_p[x]$ *с*тепені n. Використання такого представлення дає можливість ефективно проводити алгебраїчні операції в кільці, особливо операцію взяття за модулем. Проте для операції, що необхідна для канонічного підйому еліптичних кривих, а саме обчислення значення підстановки Фробеніуса, є дуже повільною. Для зменшення обчислювальної складності обчислення підстановки Фробеніуса автори методу SST в роботі [8] запропонували використовувати інше представлення кільця *p-адичних* чисел. Таке представлення дозволяє значно прискорити обчислення підстановки Фробеніуса, але вимагає певних передобчислень.

Суть використання альтернативного представлення полягає у використанні модуля Тейхмюллера. Таке представлення кільця дозволяє зменшити обчислення підстановки Фробеніуса. Так як $\Sigma(\theta)=\theta^p$ за модулем 2 та $\Sigma(\theta)$ є *(q–1)-ий* корінь одиниці в Z_q, автори роблять висновок, що $\sum(\theta)=\theta^p \bmod p$. Тому ефективне обчислення підстановки Фробеніуса зводиться до:

$$\sum\left(\sum_{i=0}^{n-1} a_i\theta^i\right)=\sum_{i=0}^{n-1} a_i\theta^{ip}, \qquad (28)$$

результат обчислень в такому випадку треба завжди приводити за модулем Тейхмюллера. Для двійкового поля характеристика p приймає значення 2.

Проте автори методів у своїх роботах пропонують використання оберненої підстановки Фробеніуса, а для двійкового поля, обчислення оберненої підстановки Фробеніуса не вимагає великої кількості обчислень при використані модуля Тейхмюллера, а передобчислення полягають в знаходженні лише одного елемента:

$$C_1(\theta)=\theta^{2^{n-1}}, \qquad (29)$$

що також є тривіальною задачею.

Проте таке використання простору не підходить для обчислення норми за аналітичним методом, а саме для обчислення логарифму (8), тобто трюки, які автори у запропонували у своїй роботі [8] для використання будуть дієві тільки при обчисленнях за модулем $f(x) \in Z_q[x]$, що є розрядженим триномом чи пентаномом за модулем p. Тому для цього після підняття еліптичної кривої і перед обчислення норми необхідно провести конвертацією елемента $\alpha \in Z_q$, щодо якого буде виконуватися операція нормування $\mathrm{N}_{Q_p/Q_p}(\alpha)$, перехід з одного базису в інший.

Для переходу з одного базису в інший необхідно побудувати матрицю переходу, детально інформацію про побудову такої матриці можна знайти у [17]. Зауважимо, що в стовпцях матриці переходу записані координати нових базисних векторів щодо старого базису. В нашому випадку, при обчислені порядку еліптичної кривої, для матриці переходу необхідно обчислити підняття Тейхмюллера для елементів $0, x, ..., x^n$. Алгоритм підняття Тейхмюллера описаний у [7, 9]. Складність такого підняття приблизно дорівнює $O(N^{\mu+1}n^{\mu})$, так як таких підйомів необхідно виконати n, то складність переходу між базисами складає $O(N^{\mu+1}n^{\mu+1})$. Після формування матриці переходу необхідно її помножити на вектор (елемент α), таке множення не вносить особливої складності при переході.

Теоретична та практична складність конвертації елементів з одного базису в інший, а також повна складність етапу нормування для проаналізованих методів наведена у Таблиці 5. Зауважимо, що нормування за результантом виконувалося без переходу до іншого базису, тобто всі операції виконувалися з модулем, що представлений у формі Тейхмюллера і в цьому разі складність обчислень більша, ніж наведена в оцінці у попередньому розділі.

Таблиця 5 – Практична складність оцінюваних методів нормування з урахуванням переходів між базисами

Степінь розширення поля d, *біт*	Алгоритм				
	Теоретична складність переходу, $O(N^{\mu+1}n^{\mu+1})$, бітових операцій	Практична складність переходу, *с*	SST метод з переходом, *с*	Результант через матрицю Сильвестра без переходу, *с*	Модифікований метод через зменшену матрицю без переходу, *с*
7	$4 \cdot 10^3$	$3{,}4 \cdot 10^{-4}$	$6{,}3 \cdot 10^{-4}$	$3{,}9 \cdot 10^{-5}$	$3{,}1 \cdot 10^{-5}$
79	10^9	$7{,}1 \cdot 10^{-1}$	$7{,}2 \cdot 10^{-1}$	$3 \cdot 10^{-2}$	$2{,}7 \cdot 10^{-2}$
107	$5{,}9 \cdot 10^9$	1,1	1,2	0,7	0,06
257	$5{,}6 \cdot 10^{11}$	29,7	29,8	1,2	1
383	$4{,}5 \cdot 10^{12}$	134,9	135	4,25	4
503	$1{,}8 \cdot 10^{13}$	312,8	313	9,9	8,9
709	10^{14}	1707,5	1708	38,6	34,4
827	$2{,}4 \cdot 10^{14}$	2798,3	2799	75,9	65,7
1031	$7{,}7 \cdot 10^{14}$	5471,3	5473	189,7	165,5

За результатами аналізу табл. 5 можна стверджувати, що практична обчислювальна складність модифікованого методу менша приблизно на 15 %, порівняно зі звичайним методом обчислення детермінанту матриці Сильвестра, навіть для іншого базису (Тейхмюллера). Якщо взяти до увагу складність переходу між базисами, то ситуація кардинально відрізняється порівняно з попереднім розділом. Так складність обчислення методів знаходження норми через результант менша від аналітичного методу для 257 біт майже у 30 разів, для 503 у 35 разів і чим далі тим вони стають більш ефективними, порівняно з аналітичним методом.

Якщо порівняти табл. 3, табл. 4 та табл. 5, то можна стверджувати, що практичні та теоретичні складності даних методів майже сходяться. Звичайно це зумовлено тим, що оцінка аналітичного методу є доволі грубою, а теоретична оцінка методів на основі результанта не враховує інші складності, що містяться в програмних реалізаціях і особливостях використання іншого модуля. Проте характер росту складності даних методів від розміру розширення базового поля спостерігається і сходиться.

Перевагою методів на основі результанта при використанні іншого модуля є можливість розпаралелювання обчислень детермінанта, в той час як аналітичний метод розпаралелити неможливо, а також на багато більша швидкодія. Фактично наша модифікація методу обчислення норми є оптимальною з точки зору складності обчислень для випадку, коли необхідно переходити між базисами для обчислення норми.

Висновки. В результаті проведених досліджень встановлено:

1. Аналітичний метод є оптимальним для свого використання, коли обчислення проводяться в оптимальному поліноміальному базисі або є передобчислена матриця переходу між базисами. В той час запропонований в цій роботі методу на основі результанта та використання зменшеної матриці Сильвестра є оптимальним при використанні базису Тейхмюллера, порівняно з аналітичним методом у цьому ж базисі. Крім того, наша модифікація методу може бути розпаралелина при виконанні обчислень, в той же час аналітичний метод не можу бути розпаралелений

2. Модифікація одного з методів, що може бути використаний в певних системних рішеннях при генерації власних (нерекомендованих у стандарті) загальних параметрів для ЕК, що визначена над двійковим полем, може бути використана для обчислення норми.

3. В роботі запропоновано використання матриці Сильвестра для обчислення результанту і відповідно до [9] норми елемента в кільці *p-адичних* чисел, а основі

цього методу запропонована наша модифікація. Для всіх алгоритмів, в тому числі і запропонованих (модифікованих) нами, було наведено та обчислено часову складність виконання. Для аналітичного методу, методів на основі результанта прорахована теоретична та оцінена практична складність обчислення норми. Показано, що теоретичні та практичні оцінки сходяться.

Список літератури:

1. *Ганзя, Р. С.* Методологія генерування сильних криптографічних загальносистемних параметрів еліптичних кривих [Текст] / *Р. С. Ганзя* // Проблеми кібербезпеки інформаційно-телекомунікаційних систем. – Київ: Київський національний університет імені Тараса Шевченка, 2017. – С. 40–44.
2. *Ганзя, Р. С.* Оцінка обчислювальної складності методів підрахунку кількості точок на еліптичній кривій [Текст] / *Р. С. Ганзя* // Системи обробки інформації. – 2016. – Вип. 8 (145). – С. 92–99.
3. *Gorbenko, I.* Examination and implementation of the fast method for computing the order of elliptic curve [Text] / *I. Gorbenko, R. Hanzia* // Eestern-European Journal of Enterprise Technologies. – 2017. – Vol. 2, Issue 9 (86). – P. 11–20. doi: 10.15587/1729-4061.2017.95194
4. *Горбенко, Ю. І.* Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем [Текст] / *Ю. І. Горбенко, Р. С. Ганзя* // Восточно-Европейский журнал передовых технологий. – 2014. – Т. 1, № 9 (67). – С. 8–16. – Режим доступа: http://journals.uran.ua/eejet/article/view/19897/18759
5. *Горбенко, І. Д.* Прикладна криптологія [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. – 868 с.
6. *Schoof, R.* Counting points on elliptic curves over finite fields [Text] / *R. Schoof* // Journal de Théorie des Nombres de Bordeaux. – 1995. – Vol. 7, Issue 1. – P. 219–254. doi: 10.5802/jtnb.142
7. *Vercauteren, F.* Computing zeta functions of curves over finite fields [Text]: dissertation for the degree of PhD / *F. Vercauteren.* – Katholieke Universiteit Leuven, 2003. – 195 p.
8. *Satoh, T.* Fast computation of canonical lifts of elliptic curves and its application to point counting [Text] / *T. Satoh, B. Skjernaa, Y. Taguch*i // Finite Fields and Their Applications. – 2003. – Vol. 9, Issue 1. – P. 89–101. doi: 10.1016/s1071-5797(02)00013-8
9. *Harley, R.* Asymptotically optimal p-adic point-counting [Electronic resource] / *R. Harley* // Listserv. – 2002. – Available at: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=NMBRTHRY&F=&S=&P=7824
10. *Skjernaa, B.* Satoh's algorithm in characteristic 2 [Text] / B. Skjernaa // Mathematics of Computation. – 2002. – Vol. 72, Issue 241. – P. 477–488. doi: 10.1090/s0025-5718-02-01434-5
11. Advances in Elliptic Curve Cryptography [Text] / *I. F. Blake, G. Seroussi, N. P. Smart* (Eds.). – NY, USA, 2005. – 281 p. doi: 10.1017/cbo9780511546570
12. *Satoh, T.* Asymptotically fast algorithm for computing the Frobenius substitution and norms over unramied extension of p-adic number fields [Text] / *T. Satoh.* – Department of Mathematics, Faculty of Science, Saitame University, 2001. – P. 1–21.
13. *Cohen, H.* Elliptic and Hyperelliptic Curve Cryptography [Text] / *H. Cohen, G. Frey.* – NW.: Chapman & Hall/CRC, 2006. – 843 p.
14. *Kedlaya, K. S.* Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology [Text] / *K. S. Kedlaya* // J. Ramanujan Math. Soc. – 2001. – Vol. 16. – P. 323–328.
15. *Moenck, R. T.* Fast computation of GCDs [Text] / *R. T. Moenck* // Proceedings of the fifth annual ACM symposium on Theory of computing – STOC '73. – 1973. doi: 10.1145/800125.804045
16. *Akritas, A. G.* Sylvester's Forgotten Form of the Resultant [Text] / *A. G. Akritas* // Fibonacci Quart. – 1993. – Vol. 31, Issue 4. – P. 325–332.
17. *Магазников, Л. И.* Линейная алгебра. Аналитическая геометрия [Текст]: уч. пос. / *Л. И. Магазников, А. Л. Магазникова*; Томский государственный университет систем управления и радиоэлектроники. – Томск, 2010. – 176 с.
18. *Bunch, J. R.* Triangular Factorization and Inversion by Fast Matrix Multiplication [Text] / *J. R. Bunch, J. E. Hopcroft* // Mathematics of Computation. – 1974. – Vol. 28, Issue 125. – P. 231. doi: 10.2307/2005828
19. *Bach, E.* Algorithmic Number Theory. Vol. 1: Efficient Algorithms [Text] / *E. Bach, J. Shalit*; Cambridge, Massachusetts. – Massachusetts Institute of Technology, 1996. – 512 p.

Bibliography (transliterated):

1. Hanzia, R. (2017). Metodolohiia heneruvannia sylnykh kryptohrafichnykh zahalnosystemnykh parametriv eliptychnykh kryvykh. Problemy kiberbezpeky informatsiino-telekomunikatsiinykh system. Kyiv: Kyivskyi natsionalnyi universytet imeni Tarasa Shevchenka, 40–44.
2. Hanzia, R. S. (2016). Otsinka obchyslyuval'noyi skladnosti metodiv pidrakhunku kil'kosti tochok na eliptychniy kryviy. Systemy obrobky informatsiyi, 8 (145), 92–99.
3. Gorbenko, I., Hanzia, R. (2017). Examination and implementation of the fast method for computing the order of elliptic curve. Eastern-European Journal of Enterprise Technologies, 2 (9 (86)), 11–21. doi: 10.15587/1729-4061.2017.95194
4. Gorbenko, I., Hanzia, R. (2014). Analysis of the possibility of quantum computers and quantum computings for cryptanalysis of modern cryptosystems. Eastern-European Journal of Enterprise Technologies, 1 (9 (67)), 8–16. Available at: http://journals.uran.ua/eejet/ article/view/19897/18759
5. Horbenko, I. D., Horbenko, Yu. I. (2012). Prykladna kryptolohiya. Kharkiv: Fort, 868.
6. Schoof, R. (1995). Counting points on elliptic curves over finite fields. Journal de Théorie Des Nombres de Bordeaux, 7 (1), 219–254. doi: 10.5802/jtnb.142
7. Vercauteren, F. (2013). Computing zeta functions of curves over finite fields. Katholieke Universiteit Leuven, 195.
8. Satoh, T., Skjernaa, B., Taguchi, Y. (2003). Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields and Their Applications, 9 (1), 89–101. doi: 10.1016/s1071-5797(02)00013-8
9. Harley, R. (2002). Asymptotically optimal p-adic point-counting. Listserv. Available at: https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L =NMBRTHRY&F=&S=&P=7824
10. Skjernaa, B. (2002). Satoh's algorithm in characteristic 2. Mathematics of Computation, 72 (241), 477–488. doi: 10.1090/s0025-5718-02-01434-5
11. Blake, I. F., Seroussi, G., Smart, N. P. (Eds.) (2005). Advances in Elliptic Curve Cryptography. NY, USA, 281. doi: 10.1017/cbo9780511546570
12. Satoh, T. (2001). Asymptotically fast algorithm for computing the Frobenius substitution and norms over unramied extension of p-adic number fields. Department of Mathematics, Faculty of Science, Saitame University, 1–21.
13. Cohen, H., Frey, G. (2006). Elliptic and Hyperelliptic Curve Cryptography. NW.: Chapman & Hall/CRC, 843.
14. Kedlaya, K. S. (2001). Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. J. Ramanujan Math. Soc., 16, 323–328.
15. Moenck, R. T. (1973). Fast computation of GCDs. Proceedings of the Fifth Annual ACM Symposium on Theory of Computing – STOC '73. doi: 10.1145/800125.804045
16. Akritas, A. G. (1993). Sylvester's Forgotten Form of the Resultant. Fibonacci Quart, 31 (4), 325–332.
17. Mahaznykov, L. Mahaznykova, A. (2010). Lyneinaia alhebra. Analytycheskaia heometryia. Tomsk, 176.
18. Bunch, J. R., Hopcroft, J. E. (1974). Triangular Factorization and Inversion by Fast Matrix Multiplication. Mathematics of Computation, 28 (125), 231. doi: 10.2307/2005828
19. Bach, E. (1996). Algorithmic Number Theory. Vol. 1: Efficient Algorithms. Massachusetts Institute of Technology, 512.

Надійшла (received) 16.06.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Вдосконалення методу нормування в кільці р-адичних чисел/ Ганзя Р. С. / Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 19(1241). – С.53–64. – Бібліогр.: 19 назв. – ISSN 2079-5459.

Совершенствование метода нормирования в кольце р-адичних чисел/ Ганзя Р. С. / Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 19(1241). – С.53–64. – Бібліогр.: 19 назв. – ISSN 2079-5459.

Improving of methods of norm computation in the ring of p-adic numbers/ Hanzia R. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 19 (1241).– P.53–64. – Bibliogr.:19. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Ганзя Роман Сергійович – Харківський національний університет радіоелектроніки, аспірант кафедри "Безпеки інформаційних технологій"; пр. Науки, 14, м. Харків, Україна, 61166; e-mail: roman.ganzya@gmail.com

Ганзя Роман Сергеевич – Харьковский национальный университет радиоэлектроники, аспирант кафедры "Безопасности информационных технологий "; пр. Науки, 14, г. Харьков, Украина, 61166;

Hanzia Roman – Kharkiv National University of Radio Electronics; PhD student of the department "Information Security Technologies"; Nauky ave., 14, Kharkiv, Ukraine, 61166; e-mail: roman.ganzya@gmail.com

УДК 004.738.2

В. А. СВЯТНИЙ, О. М. МІРОШКІН, В. В. ГРИША

РЕАЛІЗАЦІЯ ЗВ'ЯЗКУ З СИСТЕМОЮ АСКОЕ ЧЕРЕЗ GSM МЕРЕЖУ

В даній статті розглядається склад сучасних автоматизованих систем комерційного обліку електричної енергії, їх головні складові, приведені до розгляду архітектури сучасної автоматизованої системи комерційного обліку електричної енергії з трьома рівнями та двома рівнями, розглянуті сучасні засоби зв'язку автоматизованих систем контролю і обліку електричної енергії, наведено приклад каналів передачі інформації даних з використанням GSM-мережі, також за допомогою PLC технології, через виту пару і перетворювач інтерфейсів та за наявності прокладеної локальної мережі, виконано порівняння волоконно-оптичних ліній зв'язку та комутованих і виділених каналів передачі даних, детально розглянуті інтерфейси каналів зв'язку з АСКОЕ, а також розглянуто питання про проблему передачі інформації в автоматизованих системах комерційного обліку електричної енергії та запропонований один із варіантів її вирішення шляхом реалізації зв'язку з автоматизованими системами комерційного обліку електричної енергії з використанням технології GSM.

Ключові слова: автоматизована система комерційного обліку електроенергії, АСКОЕ, контроль енергоресурсів, GSM-мережа.

В данной статье рассматривается состав современных автоматизированных систем коммерческого учета электрической энергии, их главные составляющие, приведены к рассмотрению архитектуры современной автоматизированной системы коммерческого учета электрической энергии с тремя уровнями и двумя уровнями, рассмотрены современные средства связи автоматизированных систем контроля и учета электрической энергии, приведен пример каналов передачи информации по GSM-сети, также с помощью PLC технологии, через витую пару и преобразователь интерфейсов и при наличии уже созданной ранее локальной сети, выполнено сравнение волоконно-оптических каналов связи и коммутированных и выделенных каналов передачи данных, детально рассмотрены интерфейсы каналов связи с автоматизированными системами коммерческого учета электрической энергии, а также рассмотрен вопрос о проблеме передачи информации в автоматизированных системах коммерческого учета электрической энергии и предложен один из вариантов ее решения путем реализации связи с автоматизированными системами коммерческого учета электрической энергии с использованием технологии GSM.

Ключевые слова: автоматизированная система коммерческого учета электроэнергии, АСКУЭ, контроль энергоресурсов, GSM-сеть.

Composition of modern automated system of commercial electricity metering is examined in the article, the main constituents of it, three-level and two-level architectures of modern automated system of commercial electricity metering are shown, modern communication of automated system of commercial electricity metering means are considered, information transfer channels example is made for GSM-network, by means of PLC of technology, through the twisted pair and transformer of interfaces and at presence of already created earlier a local network, comparison of fibre channels of connection and switched and distinguished circuits of communication of data is executed, the interfaces of communication channels of automated system of commercial electricity metering are considered in detail and also the problem of information transfer in the automated system of commercial electricity metering is considered and the way to its decision by GSM-technology means is offered in the article.

Keywords: automated system of commercial electricity metering, control of power resources, GSM- network.

Вступ. Ключовим елементом в розвитку економіки будь-якої держави і життєво необхідним чинником існування людства у сучасному світі є електрична енергія [1]. Усі інфраструктури є споживачами електричної енергії, тому потрібне своєчасне і якісне постачання нею усіх галузей. Потреба в обліку великих потоків електроенергії при її експорті та при перетоках між енергосистемами, об'єднаними енергетичними системами та у масштабах єдиної енергетичної системи, обумовила необхідність створення систем достовірного обліку електроенергії на всіх ділянках і рівнях її виробництва, передачі й споживання.

Автоматизована система контролю і обліку електричної енергії (АСКОЕ) - це сукупність програмних і технічних засобів, спеціалізованих для автоматичного обліку електроенергії і автоматичного управління процесом електроживлення. Впровадження цієї системи дозволяє отримати точнішу інформацію про витрати споживаної електричної енергії і потужності.