The necessary and sufficient conditions for the divisibility of a point $G=(X,Y)$ of a curve $E_{a,d}$ by 2 are found. The possibility of using these curves to generate a crypto-resistant sequence of a large period is investigated.

All possible numbers of the result of the division of a point into two and the dependence of these quantities on the dividend point are studied. The necessary and sufficient conditions for the existence of 4 different preimages of a point $G=(X,Y)$ when dividing it into two are investigated. Pairing-friendly curves of prime or near-prime order are absolutely essential in certain pairing-based schemes like short signatures with longer useful life.

Key words: *elliptic curve, twisted Edwards curve, curve order, points order, Legendre symbol, square, non-square.*

Получено 21.01.2019

УДК 519.65
DOI: 10.32626/2308-5878.2019-19.155-160

В. М. Старков, д-р фіз.-мат. наук,
П. М. Томчук, д-р фіз.-мат. наук
Інститут фізики НАН України, м. Київ

ПРО ВПЛИВ ПОХИБОК ВИМІРЮВАНЬ НА ІНТЕРПРЕТАЦІЮ РЕЗУЛЬТАТІВ ЛАЗЕРНИХ ЕКСПЕРИМЕНТІВ

На основі врахування і математичного аналізу незначних апаратних похибок вимірювань розглянуті приклади їх впливу на фізичну інтерпретацію лазерних експериментальних досліджень. Проведений нами аналіз показує, що ігнорування факту наявності похибок може призвести до помилкових висновків щодо фізичної суті розглянутих оптичних явищ.

Ключові слова: *похибки вимірювань, експеримент, інтерпретація, апроксимація.*

Вступ. На принципове значення достовірності інтерпретації результатів фізичних досліджень звертали увагу видатні вчені [1, 2]. Так, в роботі [2, с. 3] сказано: «Будь-яке наукове дослідження в галузі фізики (і не тільки в галузі фізики) безсумнівно, пов'язане з інтерпретацією отриманих результатів. Таку інтерпретацію часто називають «з'ясуванням фізичного сенсу» або досяганням «розуміння» тих явищ, які досліджують. Зазвичай, інтерпретація фізичного явища відображає рівень розвитку науки в даний момент часу, і тому вона не є абсолютною, а може змінюватися з плином часу». До останнього зауваження можна лише додати, що інтерпретація відображає, крім усього іншого, рівень інтелекту, освіти, наукового досвіду і т.д. дослідника, який її реалізує. Інтерпретація результатів наукового фізич-

ного експерименту неминуче обумовлена тим, що дослідник повинен мати чітке уявлення про взаємодію всіх складових елементів експериментального процесу. Дуже важливою якісною обставиною в цій роботі є обов'язкове врахування наявності в результатах експерименту похибок вимірювань, оскільки експеримент завжди проводять на реальних установках. Якраз на цій множині даних з сукупністю різного роду похибок виникають нерідко серйозні проблеми.

Математична інтерпретація даних оптичного експерименту. Умовно наш приклад пов'язаний з експериментальними дослідженнями ефектів оптичного обмеження в тонких наноструктурних плівках різних політипів карбіду кремнію. Це середовище є перспективним для використання в екстремальних умовах високих і низьких температур, при значних радіаційних навантаженнях і в хімічно активній атмосфері [3, с. 91]. Результати досліджень показали, зокрема, що в зразку карбіду кремнію, який характеризується в основному аморфною фазою, ефект оптичного обмеження, як на основній довжині хвилі генерації неодимового лазера (λ = 1064 нм), так і на його другій гармоніці (λ = 532 нм), не був виявлений. Аналогічний результат був отриманий і для зразка, який завдяки додатковій обробці відпалом складався майже на 100 % з кристалічної фази (3C) нанорозмірного карбіду кремнію. З цих результатів випливає, що залежність інтенсивності випромінювання, що пройшло через зразок, від інтенсивності падаючого випромінювання носить майже лінійний характер для аморфного і 100 % кристалічного зразка.

Оскільки метою подальшого викладу є виявлення інтерпретації без строгого врахування похибки реєстрованих даних, то будемо використовувати інші лінійні залежності подібного роду, але з більшим на порядок числом експериментальних точок і з більш яскраво вираженими похибками вимірювань [4, с. 485–486].

На рис. 1, а показано типову залежність (експеримент 1) відносної величини зареєстрованого сигналу (наприклад, проходження лазерного пучка через обмежуючу діафрагму за умови відсутності зразка) від вхідного сигналу $u_\delta(x) = I_\delta^{(out)} / I_{\max}$, $x = I^{(in)} / I_{\max}$. Аналогічну залежність (експеримент 2) відносної величини сигналу повного пропускання зразка від інтенсивності лазерного випромінювання приведено на рис. 1, b: $u_{\delta s}(x) = \tilde{I}_\delta^{(out)} / I_{\max}$. З достатнім ступенем впевненості можна стверджувати, що обидві залежності носять лінійний характер. Дійсно, апроксимуючи експериментальні дані лінійними функціями, отримаємо:

$$\hat{u}_\delta(x) = a_1 + b_1 x;\ a_1 = 0.00485;\ b_1 = 1.227; \quad (1)$$

$$\hat{u}_{\delta s}(x) = a_2 + b_2 x;\ a_2 = -\,0.00175;\ b_2 = 1.078. \quad (2)$$

Максимальні похибки наближення в першому і другому випадку виявляються рівними відповідно $\delta\hat{u} = 0.015$, $\delta\hat{u}_s = 0.012$.

Результати апроксимації (1), (2) показані графіками на рис. 2.

Якщо наблизити результати експерименту без зразка (рис. 1) поліномом третього степеню:

$$\bar{u}_\delta(x) = a_3 + b_3 x + c_3 x^2 + d_3 x^3;$$

$$a_3 = -0.0148;\ b_3 = 1.533;\ c_3 = -1.167;\ d_3 = 1.266, \qquad (3)$$

то отримаємо максимальну похибку наближення, що дорівнює $\delta\bar{u} = 0.0145$, тобто менша, ніж в разі лінійної апроксимації.

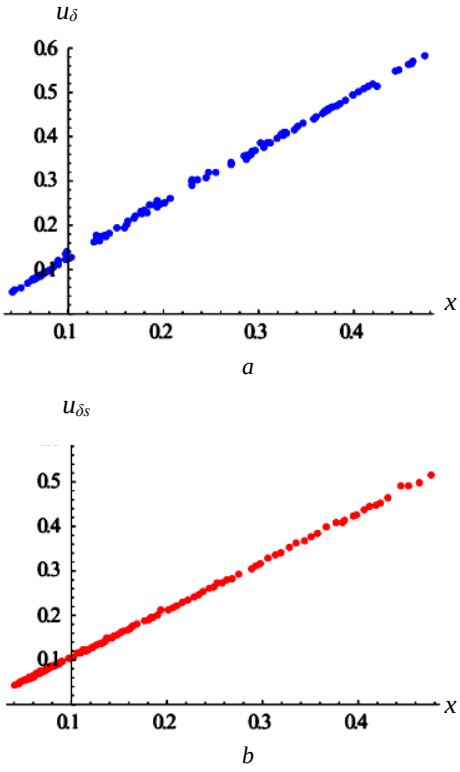

Рис. 1. *Залежність інтенсивності лазерного випромінювання, що пройшло через обмежуючу діафрагму за умови відсутності зразка* (*a*), *та інтенсивності лазерного випромінювання, що пройшло через зразок* (*b*), *від інтенсивності падаючого випромінювання*

Слід зазначити принципове значення того факту, що в результаті всіх наближень (1)–(3) коефіцієнти a_i $(i = 1, 2, 3)$ виявилися ненульо-

вими. Інакше кажучи, при відсутності сигналу на вході в систему вимірювальна апаратура фіксує в першому і другому варіанті експерименту присутність сигналу. Цей сигнал є ніщо інше, як похибка моделювання на початку координат

$$\delta u(0) = u_\delta(0) - u(0) \neq 0 . \qquad (4)$$

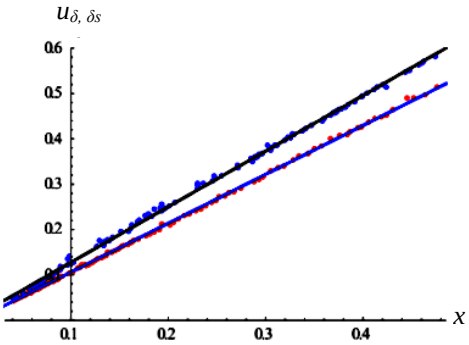

Рис. 2. *Апроксимації експериментальних даних лінійними функціями*

Ігнорування цього факту може призвести до невірної фізичної інтерпретації експериментальних досліджень. Справа в тому, що зіставлення результатів вимірювань у другому експерименті з даними в першому здійснюють нерідко шляхом діленням одних даних на другі: $\left(\hat{u}_{\delta s}(x) / \hat{u}_\delta(x)\right)$. Такий варіант можливий, наприклад, при наявності ідеальної вимірювальної апаратури, яка виключає будь-які похибки. За ідеальних умов усі експериментальні точки лежать строго на прямій, яка, в свою чергу, проходить через початок координат.

Пояснимо сказане простими викладками. Нехай $a_1 = 0$ и $a_2 = 0$, тоді

$$\hat{u}_{\delta s}(x) / \hat{u}_\delta(x) = \hat{b}_2 x / \hat{b}_1 x = const \ \ (\hat{b}_1 \neq 0) .$$

Підкреслимо: або це ідеальний варіант, або в процесі попередньої обробки експериментальні дані наближаються лінійними функціями $u_{\delta i}(x) = b_i x$. Зрозуміло, що мова йде про експерименти, результати яких подібні представленим на рис. 1 та 2.

Розглянемо перший, досить простий, але реальний випадок, коли дані вимірювань супроводжують похибки, але пряма лінія перших вимірів проходить строго через нуль ($a_1 = 0$), тобто при відсутності сигналу на вході в систему відсутній і спостережуваний сигнал. Нехай всі інші коефіцієнти мають попередні значення з експериментів 1 і 2. Тоді

$$v_1(x) = \hat{u}_{\delta s}(x) / \tilde{u}_\delta(x) = (a_2 + b_2 x) / (b_1 x) =$$

$$= b_2 / b_1 + a_2 / (b_1 x) = \alpha_1 + \beta_1 x^{-1}, \ \ \alpha_1 = 0.879, \ \beta_1 = -0.00143,$$

так, що отримана звичайна гіпербола.

Якщо розглядати варіант, коли всі коефіцієнти з (1) і (2) відмінні від нуля, то і в цьому випадку буде отримана гіперболічна залежність. Можна тепер уявити, що деякому «абстрактному експериментатору», який з різних причин залишає без уваги (4), більш цікавий варіант, коли результати першого експерименту апроксимовані поліномом третього степеня (3). Тим більше, функції $v_1(x)$ и $v_2(x)$ поводять себе в околі нуля своєрідно. В результаті виходить така функція $v_3(x)$, графічне зображення якої (рис. 3, а) може викликати спокусу пошуку якогось «глибокого» фізичного сенсу.

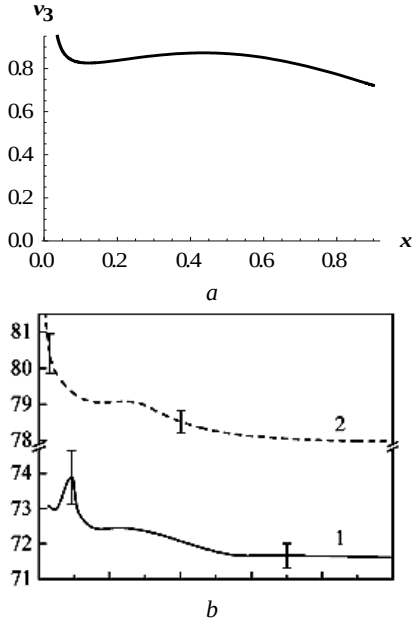

Рис. 3. *Графічне представлення функції* $v_3(x)$ (*a*) *та її аналога* (*b, крива 2 [5, с. 98]*)

Справа в тому, що якщо розкласти $\bar{u}_\delta(x)$ (17) на прості множники

$$\bar{u}_\delta(x) = (x - 0.00972)(1.266\,x^2 - 1.155\,x + 1.522),$$

то можна побачити, що значення $x^* = 0.00972$ є особливою точкою функції

$$v_3(x) = \hat{u}_{\delta s}(x) / \bar{u}_\delta(x) = (1.078x - 0.00175) \times$$
$$\times[(x - 0.00972)(1.266\,x^2 - 1.155\,x + 1.522)]^{-1}$$

і її похідних. Наявність полюса визначає характер поведінки розглянутої функції $v_3(x)$. Щоб уникнути невірної інтерпретації результа-

тів експерименту можна рекомендувати замість поділу функцій використовувати відносини їх похідних $\left(\hat{u}'_{\delta s}(x)/\hat{u}'_{\delta}(x) = b_2/b_1\right)$.

Як приклад такого роду «глибокого» фізичного сенсу можна вказати на результати роботи [5, с. 98] (рис. 3), де крива 2 демонструє наявність фізичного ефекту НЛО. Так що основний результат роботи був сформульований як видатне досягнення дослідника [6, с. 35]: «Вперше було спостережено ефект гігантського нелінійно-оптичного (НЛО) відгуку в пористих шарах нанокристалів TiO2 анатаз модифікації, що на шість порядків перевищує відгук об'ємного матеріалу».

Висновки. На конкретних прикладах результатів наукових експериментальних досліджень ми показали, що апроксимація експериментальних залежностей оптичного експерименту поліномами (як це часто роблять) при неуважному ставленні до наявності похибок у даних експерименту (особливо в околі початку координат) може призвести до невірної фізичної інтерпретації отриманих результатів.

Список використаних джерел:

1. Гейзенберг В. К. Что такое «понимание» в теоретической физике. *Природа.* 1971. № 4. С. 75–77.
2. Давыдов А. С. Интерпретация результатов научных исследований в области физики. *Препринт ИТФ. 80. I3IP.* 1980. 28 с.
3. Borshch A. A., Brodyn M. S., Starkov V. N. et al. Broadband optical limiting in thin nanostructured silicon carbide films and its nature. *Optics Communications.* 2016. № 364. P. 88–92.
4. Starkov V. N., Borshch A. A., Gandzha I. S., Tomchuk P. M. Some Examples of Seemingly Plausible Interpretation of Experimental Results. *Ukr. J. Phys.* 2017. Vol. 62. № 6. P. 481–488.
5. Gayvoronsky V., Galas A., Shepelyavyy E. et al. Giant nonlinear optical response of nanoporous anatase layers. *Appl. Phys. B* 80. 2005. P. 97–100.
6. Гайворонский В. Я. Дослідження нелінійно-оптичних властивостей композитів на основі пористих напівпровідників та наноструктурованих діелектриків. Автореф. дис. … д-ра фіз.-мат. наук. Інститут фізики НАН України. Київ, 2015. 38 с.

ON THE EFFECT OF MEASUREMENT ERRORS ON THE INTERPRETATION OF LASER EXPERIMENTAL RESULTS

On the basis of accounting and mathematical analysis of minor instrumental measurement errors, examples of their influence on the physical interpretation of laser experimental studies are considered. Our analysis shows that ignoring the fact of errors may lead to erroneous conclusions regarding the physical essence of the considered optical phenomena.

Key words: *measurement errors, experiment, interpretation, approximation.*

Одержано 11.02.2019