

- а) 2^{999} ; д) 203^{203203} ;
 б) 3^{999} ; е) $14^{14^{14}}$;
 в) 2^{341} ; ж) 9^{9^9} ;
 г) 289^{289} ; ж) 7^{9^9} .

11.17. Нехай $F_n = 2^{2^n} + 1$ — число Ферма, де $n = 0, 1, 2, \dots$
Довести, що:

- а) $F_5 = 6411$;
 б) число F_n закінчується цифрою 7 при всіх n , крім $n=0$
і $n=1$.

§ 12. Класи лишків, повна і зведені системи лишків за даним модулем

Література

- [1] — § 15, с. 166—168, § 16, с. 168—170;
 [2] — § 15, с. 169—171, § 16, с. 171—173;
 [3] — гл. 12, § 2, 3, с. 399—404;
 [10] — гл. III, § 4, 5, с. 45—46;
 [11] — гл. 8, 9, с. 77—92;
 [12] — гл. II, § 2, 3, с. 43—51;
 [13] — § 16—18, с. 66—78.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Відношення конгруентності за даним модулем m є бінарним відношенням еквівалентності на множині цілих чисел Z . Класи еквівалентностей називають **класами лишків за даним модулем**. **Лишком** (або представником) класу за модулем m називають будь-яке число цього класу. Кільце цілих чисел Z розкладається на m класів лишків. До класу лишків, який містить число a , належать усі цілі числа x виду $x = a + mt$, де $t \in Z$. Цей клас позначатимемо символом $K_a^{(m)}$, причому, якщо йдеться тільки про класи лишків за тим самим модулем m , то можна писати K_a . Число a називають **представником класу лишків** $K_a^{(m)}$.

Представником класу лишків $K_a^{(m)}$ може бути будь-який елемент цього класу, тобто $K_a^{(m)} = K_b^{(m)}$, якщо $b \in K_a^{(m)}$. Якщо $K_a^{(m)} \cap K_b^{(m)} \neq \emptyset$, то $K_a^{(m)} = K_b^{(m)}$. Якщо $d > 1$, то $K_a^{(m)} = K_a^{(dm)} \cup K_{(a+m)}^{(dm)} \cup K_{(a+2m)}^{(dm)} \cup \dots \cup K_{(a+(d-1)m)}^{(dm)}$:

$$K_a^{(m)} + K_b^{(m)} = K_{a+b}^{(m)}, \quad K_a^{(m)} K_b^{(m)} = K_{ab}^{(m)}.$$

Множина всіх класів лишків за модулем m відносно додавання класів утворює комутативну групу, її називають **групою класів лишків**.

Множина класів лишків кільца цілих чисел за даним модулем m утворює комутативне кільце з одиницею, його позначають Z_m .

Якщо m — складене число, то в Z_m є дільники нуля, причому, якщо $m = m_1 m_2$, то зокрема,

$$K_{m_1}^{(m)} K_{m_2}^{(m)} = K_{\phi}^{(m)}, \text{ де } K_{m_1}^{(m)} \neq K_{\phi}^{(m)} \text{ і } K_{m_2}^{(m)} \neq K_{\phi}^{(m)}.$$

Якщо m — просте число, то Z_m — скінченне поле.

Повною системою лишків за модулем m називають будь-яку систему лишків, утворену з m чисел, взятих по одному з кожного класу лишків.

Існують такі основні повні системи лишків:

¹ Це було доведено ще Л. Ейлером (1707—1783).

- a) повна система найменших невід'ємних лишків;
- б) повна система найменших за абсолютною величиною лишків;
- в) повна система найменших натуральних лишків.

Якщо $(a, m) = 1$, то клас $K_a^{(m)}$ називають **взаємно простим** з модулем m .

Зведену системою лишків за модулем m називають будь-яку систему лишків, утворену з $\varphi(m)$ чисел, взятих по одному з кожного класу, взаємно простого з модулем m .

Якщо $(a, m) = 1$, b — довільне ціле число, а x пробігає повну систему лишків за модулем m , то й вираз $ax + b$ також пробігає деяку повну систему лишків за модулем m (не обов'язково ту саму).

Якщо $(a, m) = 1$, а x пробігає зведену систему лишків за модулем m , то лінійна форма ax також пробігає деяку зведену систему лишків за модулем m (не обов'язково ту саму).

Множина класів лишків за модулем m , взаємно простих з m , утворює відносно множення класів комутативну групу, її називають **мультиплікативною групою класів лишків**, взаємно простих з модулем.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Чи утворює повну систему лишків за модулем 8 система чисел

$$S = \{-7, 2, 16, 20, 27, 39, 46, -3\}?$$

Розв'язання. Щоб визначити, чи є деяка система чисел повною системою лишків за дійким модулем m , треба: 1) впевнитися, що цих чисел є m , 2) показати, що всі вони між собою попарно неконгруентні за модулем m . При цьому доцільно замінити кожне з даних чисел конгруентним йому найменшим невід'ємним числом (це неважко зробити, знайшовши остатчу від ділення заданого числа на модуль).

У розглядуваному прикладі маємо: 1) чисел у системі є 8; 2) $-7 \equiv 1 \pmod{8}$, $2 \equiv 2 \pmod{8}$, $16 \equiv 0 \pmod{8}$, $20 \equiv 4 \pmod{8}$, $27 \equiv 3 \pmod{8}$, $39 \equiv 7 \pmod{8}$, $46 \equiv 6 \pmod{8}$, $-3 \equiv 5 \pmod{8}$. Дістали нову систему 1, 2, 0, 4, 3, 7, 6, 5, яка є повною системою лишків за модулем 8.

Зауваження. 1. Якщо модуль m є невелике число, можна знайти всі попарні різниці заданих чисел і довести їхню подільність на m . Якщо жодна з різниць не ділиться на m , то задана сукупність чисел є повною системою лишків за модулем m , у протилежному разі — не є нею.

2. Замінивши кожне число системи S його остаточею від ділення на 8, визначимо, до якого класу $K_a^{(8)}$ належить кожне число із системи S , а саме $-7 \in K_1^{(8)}$, $2 \in K_2^{(8)}$, $16 \in K_0^{(8)}$, $20 \in K_4^{(8)}$, $27 \in K_3^{(8)}$, $39 \in K_7^{(8)}$, $46 \in K_6^{(8)}$, $-3 \in K_5^{(8)}$.

Оскільки всі числа з S належать до різних класів за модулем 8 і всі класи мають представників у цій системі, то S — повна система лишків за модулем 8.

2. Показати, що коли x пробігає зведену систему лишків за модулем 10, то x^3 пробігає зведену систему лишків за модулем 10.

Розв'язання. Відомо, що числа зведеній системи лишків взаємно прості з модулем. Взаємно простими з 10 є лише такі цілі числа, які закінчуються цифрами 1, 3, 7, 9. Четвірки 3 таких чисел попарно неконгруентні між собою за модулем 10, а оскільки $\varphi(10) = \varphi(2 \cdot 5) = 2 \cdot 5 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$, то S — зведеній системі лишків за модулем 10. Нехай x пробігає довільну зведену систему лишків S за модулем 10. Якщо числа системи S , що закінчуються цифрами 1, 3, 7, 9, піднести до куба, то дістанемо систему S' чисел, які закінчуються цифрами 1, 7, 3, 9. Цю систему й пробігає x^3 . Система S' утворює також зведену систему лишків за модулем 10, оскільки: а) чисел у системі є $4 = \varphi(10)$, б) усі числа системи S' попарно неконгруентні між собою за модулем 10; в) усі числа системи S' взаємно прості з числом 10.

3. У множині класів лишків за модулем 15 знайти:

- а) усі дільники нуля;
- б) усі дільники одиниці;

в) клас, протилежний класу $K_7^{(15)}$;

г) клас, обернений до класу $K_{11}^{(15)}$.

Розв'язання. а) Оскільки дільником нуля є кожен клас $K_a^{(15)}$, для якого знайдеться такий клас $K_x^{(15)}$, що $K_a^{(15)} \cdot K_x^{(15)} = K_0^{(15)}$, де $K_a^{(15)} \neq K_0^{(15)} \neq K_x^{(15)}$, тобто такий клас $K_x^{(15)}$, що $ax \equiv 15$, де $1 < a, x < 14$, то фактично дільниками нуля є всі ті класи $K_a^{(15)}$, в яких представник a не взаємно простий з 15. Отже, дільниками нуля є такі класи: $K_3^{(15)}, K_5^{(15)}, K_6^{(15)}, K_9^{(15)}, K_{10}^{(15)}, K_{12}^{(15)}$. б) Аналогічні міркування для дільників одиниць показують, що дільниками одиниць є всі ті класи $K_a^{(15)}$, в яких представник a взаємно простий з 15. Справді, якщо $(a, 15) = 1$, то знайдуться такі цілі числа u і v , що $au + 15v = 1$. Тоді $K_{au+15v} = K_1$, проте $K_{au+15v} = K_{au} + K_{15v}$, а $K_{15v} = K_0$, $K_{au} = K_a \cdot K_u$. Отже, $K_a \cdot K_u = K_1$. Звідси, зокрема, $(K_a)^{-1} = K_u$, тобто ми вивели формулу для знаходження класу, оберненого до класу K_a , якщо $(a, 15) = 1$.

Випишемо дільники одиниць: $K_1^{(15)}, K_2^{(15)}, K_4^{(15)}, K_7^{(15)}, K_8^{(15)}, K_{11}^{(15)}, K_{13}^{(15)}, K_{14}^{(15)}$.

в) Знайдемо такий клас $K_x^{(15)}$, що $K_7^{(15)} + K_x^{(15)} = K_0^{(15)}$. Оскільки $K_7^{(15)} + K_x^{(15)} = K_{7+x}^{(15)}$, то шукатимемо таке ціле число x , що $7 + x \equiv 15$. Найменшим таким числом є 8. Отже, $x = 8$ і тому $-K_7^{(15)} = K_8^{(15)}$.

г) Знайдемо такий клас $K_u^{(15)}$, що $K_{11}^{(15)} \cdot K_u^{(15)} = K_1^{(15)}$. Оскільки $(11, 15) = 1$, то, згідно з пунктом б), цей клас можна знайти, знайшовши спочатку за допомогою алгоритму Евкліда число u . До чисел 11 і 15 застосуємо алгоритм Евкліда. Маємо:

$$\begin{aligned} 15 &= 11 \cdot 1 + 4, \\ 11 &= 4 \cdot 2 + 3, \\ 4 &= 3 \cdot 1 + 1. \end{aligned}$$

Звідси

$$\begin{aligned} 4 &= 15 - 11 \cdot 1, \\ 3 &= 11 - 4 \cdot 2, \\ 1 &= 4 - 3 \cdot 1. \end{aligned}$$

Тоді

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) \cdot 1 = 11 \cdot (-1) + 4 \cdot 3 = \\ &= 11 \cdot (-1) + (15 - 11 \cdot 1) \cdot 3 = 11 \cdot (-4) + 15 \cdot 3. \end{aligned}$$

Отже, $u = -4$, а $K_u^{(15)} = K_{-4}^{(15)}$.

Оскільки $K_{-4}^{(15)} = K_{11}^{(15)}$, то $\left(K_{11}^{(15)}\right)^{-1} = K_{11}^{(15)}$, тобто клас $K_{11}^{(15)}$ є оберненим до себе.

Зауваження

1. У подальшому, знайшовши дільники нуля (дільники одиниці), говорити- memo, що відмінні від дільників нуля і самого нуля елементи є дільниками одиниці (відмінні від дільників одиниці і від нуля елементи є дільниками нуля).

2. У пунктах а) і б), не обмежуючись тільки переліком дільників нуля та одиниці, можна виписати відповідні конкретні пари. У розглянутому прикладі такими парами відповідно є:

$$K_3^{(15)} \text{ і } K_5^{(15)}, \quad K_6^{(15)} \text{ і } K_5^{(15)} \text{ і т. д.,}$$

$$K_8^{(15)} \text{ і } K_8^{(15)}, \quad K_4^{(15)} \text{ і } K_4^{(15)} \text{ і т. д.}$$

8. Клас $K_u^{(m)}$, обернений до класу $K_a^{(m)}$, можна іноді швидко знаходити усно, підбираючи таке число u , щоб добуток $a \cdot u$ при діленні на m давав остатчу 1.

Так для класу $K_{11}^{(15)}$ класи $K_1^{(15)}, K_2^{(15)}, K_4^{(15)}, K_7^{(15)}, K_8^{(15)}$ не підійшли б, оскільки числа $1 \cdot 11 = 11$, $2 \cdot 11 = 22$, $4 \cdot 11 = 44$, $7 \cdot 11 = 77$, $8 \cdot 11 = 88$ при діленні на 15 дають остачу, відмінну від 1. При цьому, звичайно, дільники нуля $K_3^{(15)}, K_5^{(15)}, K_6^{(15)}, K_9^{(15)}, K_{10}^{(15)}$ не випробовуються, бо вони вже дільниками однині не можуть бути. Оскільки $11 \cdot 11 = 121$ і $121 = 15 \cdot 8 + 1$, то $(K_{11}^{(15)})^{-1} = K_{11}^{(15)}$.

4. Для знаходження класу $(K_a^{(m)})^{-1}$, оберненого до класу $K_a^{(m)}$, існує ще один спосіб. Нехай $(a, m) = 1$, у протилежному разі клас $K_a^{(m)}$ взагалі не має оберненого класу. Нехай P_{n-1} — чисельник передостаннього підхідного дробу $\frac{P_{n-1}}{Q_{n-1}}$ для числа $\frac{m}{a}$, $\frac{m}{a} = \frac{P_n}{Q_n}$. Оскільки $\frac{m}{a}$ — нескоротний дріб, то $m = P_n$, $a = Q_n$. За однією з властивостей підхідних дробів маємо

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n-1}}{Q_{n-1} \cdot Q_n}.$$

Отже,

$$\frac{m}{a} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n}{Q_{n-1} \cdot Q_n}.$$

Звідси

$$Q_{n-1} \cdot m - aP_{n-1} = (-1)^{n-1}.$$

Тоді

$$a(-1)^n P_{n-1} \equiv 1 \pmod{m}.$$

Згідно з цією конгруенцією, клас $K_{(-1)^n P_{n-1}}^{(m)}$ є оберненим до класу $K_a^{(m)}$.

Отже,

$$(K_a^{(m)})^{-1} = K_{(-1)^n P_{n-1}}^{(m)}.$$

Для розглянутого прикладу маємо (табл. 12), де $m = 15$, $a = 11$, $n = 3$, $P_{n-1} = P_2 = 4$. Тоді

$$(K_{11}^{(15)})^{-1} = K_{(-1)^3 \cdot 4}^{(15)} = K_{-4}^{(15)} = K_{11}^{(15)}.$$

Таблиця 12

i	-1	0	1	2	3
q_i	-	1	2	1	3
P_i	1	1	3	4	15
Q_i	0	1	2	3	11

Задачі

12.1. Замінити найменшим невід'ємним і найменшим за абсолютною величиною лишками такі числа:

- | | |
|-----------------------|-----------------------|
| а) 70 за модулем 32; | г) 333 за модулем 67; |
| б) 327 за модулем 30; | д) 586 за модулем 13; |
| в) 184 за модулем 16; | е) 799 за модулем 99; |

- е) 14 за модулем 15; л) 1000 за модулем — 17;
 ж) 5353 за модулем 781; м) 501 за модулем 503;
 з) —337 за модулем 56; н) —700 за модулем — 51.
 к) 337 за модулем — 56;

12.2. Знайти повну систему найменших невід'ємних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.3. Знайти повну систему найменших за абсолютною величиною лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.4. Знайти повну систему найменших натуральних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.5. Знайти повну систему найбільших недодатніх лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.6. Знайти повну систему найбільших від'ємних лишків за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.7. Знайти хоч одну довільну повну систему лишків, відмінну від знайдених у задачах 12.2—12.6, за модулем: а) 1; б) 2; в) 3; г) 4; д) 5; е) 6; є) 7; ж) 8; з) 9; к) 10; л) 12; м) 15; н) 20.

12.8. Знайти відповідні зведені системи лишків для задач 12.2—12.7.

12.9. Чи утворюють повну систему лишків за модулем m такі числа:

- а) 25, —20, 16, 54, —21, 26, 37, —17, якщо $m=8$;
- б) 25, —9, —6, 420, —18, 30, 6, якщо $m=7$;
- в) —46, —45, 37, 32, —48, —40, якщо $m=6$;
- г) 43, 25, —23, 28, —50, —40, 31, якщо $m=7$;
- д) —261, —130, 170, 313, 973, 1000, 55, 1668, якщо $m=8$;
- е) 605, —189, 242, —311, 143, 40, —51, 194, якщо $m=8$;
- ї) 809, 402, 1616, 220, 227, 439, 446, якщо $m=8$;
- ж) 921, 92, —18, 28, —109, 40, —22, —2, 15, якщо $m=9$;
- з) 134, 128, —19, 37, 28, —23, —32, 5, 41, —35, —33, якщо $m=11$;
- к) 39, 66, 30, 19, —11, 55, 31, 46, 25, 47, 50, 35, 101, якщо $m=13$?

12.10. Чи утворюють зведену систему лишків за модулем m такі числа:

- а) 19, —1, 25, —19, якщо $m=8$;
- б) 19, 95, 29, 49, —20, —64, 27, якщо $m=9$;
- в) 13, —13, 29, —29, якщо $m=10$;
- г) 19, 35, 25, —19, якщо $m=12$;
- д) —11, —55, —29, 35, якщо $m=12$;
- є) —181, 231, 413, —349, якщо $m=12$?

12.11. Довести, що:

- а) коли x пробігає повну систему лишків за модулем 11, то й $3x+2$ теж пробігає повну систему лишків за модулем 11;
- б) коли x пробігає повну систему лишків за модулем 10, то й x^5 пробігає повну систему лишків за модулем 10;
- в) система чисел $2, 4, \dots, 2t$ становить повну систему лишків за модулем t , якщо t непарне;
- г) члени арифметичної прогресії $a, a+d, \dots, a+d(n-1)$ утворюють повну систему лишків за модулем n , якщо $(d, n)=1$;
- д) коли $(a, b)=1$, x пробігає повну систему лишків за модулем b , y пробігає повну систему лишків за модулем a , а c — будь-яке число, то $ax+by+c$ пробігає повну систему лишків за модулем ab ;
- е) коли $t = a_1a_2\dots a_s$, де всі a_i попарно взаємно прості, $m_i = \frac{t}{a_i}$, $i = 1, 2, \dots, s$, c — довільне ціле число, x_i пробігають відповідно повні системи лишків за модулем m_i , то $m_1x_1 + m_2x_2 + \dots + m_sx_s + c$ пробігає повну систему лишків за модулем t ;
- ж) система чисел $0, 2^1, 2^2, \dots, 2^{10}$ утворює повну систему лишків за модулем 11;
- ж) вираз $3x + 7y$ пробігає повну систему лишків за модулем 21, якщо $x = 0, 1, 2, 3, 4, 5, 6$, а $y = 0, 1, 2$;
- з) повну систему лишків за модулем $m_1m_2\dots m_s$ пробігає вираз $x_1 + m_1x_2 + m_1m_2x_3 + \dots + m_1m_2\dots m_{s-1}x_s$, якщо m_1, m_2, \dots, m_s — натуральні, попарно взаємно прості числа, а x_1, x_2, \dots, x_s пробігають повні системи лишків за модулем m_1, m_2, \dots, m відповідно.

12.12. Довести, що:

- а) коли x пробігає зведену систему лишків за модулем 7, то $\bar{10}x$ пробігає зведену систему лишків за модулем 7;
- б) коли x пробігає зведену систему лишків за модулем 9, то $\bar{7}x^5$ теж пробігає зведену систему лишків за модулем 9;
- в) числа $6t-1$, і $6t+1$ при кожному цілому t утворюють зведену систему лишків за модулем 6;
- г) система чисел $\pm 1, \pm 2, \dots, \pm \frac{p-3}{2}, \frac{p-1}{2}$ є зведену системою лишків за непарним простим модулем p ;
- д) система чисел $3^1, 3^2, 3^3, 3^4, 3^5, 3^6$ утворює зведену систему лишків за модулем 7;
- е) система чисел $5^1, 5^2, 5^3, 5^4, 5^5, 5^6$ утворює зведену систему лишків за модулем 7;
- ж) коли числа $ax_1, ax_2, \dots, ax_{\varphi(m)}$ утворюють зведену систему лишків за модулем m , то відповідні числа $x_1, x_2, \dots, x_{\varphi(m)}$ також утворюють зведену систему лишків за модулем m ;
- ж) якщо $(a, m) = 1$, $b \equiv 0 \pmod{m}$ і x пробігає зведену систему лишків за модулем m , то $ax+b$ також пробігає зведену систему лишків за модулем m ;
- з) якщо $(a, m) = d$ і x пробігає зведену систему лишків за модулем $\frac{m}{d}$, то й $\frac{a}{d}x$ також пробігає зведену систему лишків за модулем $\frac{m}{d}$;

к) $K_{ap-1}^{(p)} = K_1^{(p)}$, де p — просте число, a не ділиться на p .

12.13. Об'єднанням яких класів лишків є класи лишків:

а) $K_1^{(6)}, K_3^{(6)}, K_5^{(6)}$ за модулем 48;

б) $K_1^{(13)}, K_3^{(13)}, K_5^{(13)}, K_7^{(13)}$ за модулем 52;

в) $K_2^{(10)}, K_3^{(10)}, K_5^{(10)}, K_9^{(10)}$ за модулем 30.

13.14. Знайти класи лишків, обернені до таких класів:

а) $K_2^{(3)}$; б) $K_3^{(4)}$; в) $K_3^{(5)}$; г) $K_5^{(7)}$;

д) $K_7^{(8)}$; е) $K_5^{(9)}$; е) $K_7^{(10)}$; ж) $K_5^{(11)}$;

з) $K_{57}^{(61)}$; к) $K_{196}^{(501)}$; л) $K_{190}^{(501)}$; м) $K_{233}^{(1498)}$; и) $K_{501}^{(1993)}$.

§ 13. Теореми Ейлера і Ферма

Література

[1] — § 16, с. 174—175;

[2] — § 16, с. 178—179;

[3] — гл. 12, § 3, с. 408—409;

[10] — гл. 3, § 6;

[11] — гл. 2, с. 96—106;

[12] — гл. II, § 5, с. 57—60;

[14] — § 19, с. 79—80.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Теорема Ейлера. Якщо $m > 1$ і $(a, m) = 1$, то

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Теорема Ферма (мала теорема Ферма). Якщо число p просте і $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$.

Наслідок. Якщо p — просте число, a — будь-яке ціле число, то $a^p \equiv a \pmod{p}$.

ПРИКЛАДИ РОЗВ'ЯЗУВАННЯ ЗАДАЧ

1. Знайти остаточу від ділення: а) 223^{2123} на 52; б) 264^{1020} на 138.

Розв'язання. а) Якщо треба знайти остаточу від ділення a^s на m , де $(s, m) = 1$ і $s > \varphi(m)$, то s можна подати у вигляді (за теоремою про ділення остаточою): $s = \varphi(m)q + r$, де $0 < r < \varphi(m)$. Оскільки $a^{\varphi(m)} \equiv 1 \pmod{m}$, то

$$a^s = a^{\varphi(m)q+r} = (a^{\varphi(m)})^q \cdot a^r \equiv a^r \pmod{m},$$

де a^r може бути значно меншим, ніж a^s .

У цьому разі маємо

$$52 = 2^2 \cdot 13, \quad \varphi(52) = 2^2 \cdot 13 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) = 24,$$

$$223 = 52 \cdot 4 + 15, \quad 2123 = 24 \cdot 88 + 11.$$

Тоді

$$223^{2123} = (52 \cdot 4 + 15)^{24 \cdot 88 + 11} \equiv 15^{11} = 15^9 \cdot 15^2 = (15^3)^3 \cdot 225 \equiv \\ \equiv (3375)^3 \cdot 17 \equiv (-5)^3 \cdot 17 \Rightarrow (-125) \cdot 17 \equiv (-21) \cdot 17 = -357 \equiv 7 \pmod{52}.$$

Отже, 223^{2123} при діленні на 52 дає остаточу 7.

б) Якщо $(a, m) \neq 1$ і $(a^s, m) = d > 1$, то знаходимо спочатку таке найменше k , що $a^k \equiv d$. Тоді $a^k = a_1d$, $m = m_1d$, де вже $(a, m_1) = 1$. Позначимо через x остаточу від ділення a^s на m . Тоді

$$x \equiv a^s = a^{s-k} \cdot a^k = a^{s-k} \cdot a_1d \pmod{m_1, d}.$$