1.

1. Теорема про ділення з остачею (з доведенням).
2. Теорема про найпростіші властивості відношення подільності (з доведенням).
3. Власні і невласні дільники. Прості і складені числа. Твердження про подільність кожного числа на деяке просте число (з доведенням).
4. Теорема про розклад на прості множники (з доведенням).
5. Теорема Евкліда (з доведенням).
6. Решето Ератостена.
7. Найбільший спільний дільник (НСД), теорема про його існування (з доведенням) і наслідок з неї.
8. Критерій взаємної простоти двох чисел (з доведенням). Твердження про взаємно прості числа (з доведенням).
9. Найменше спільне кратне (НСК), теорема про зв'язок між НСД і НСК (з доведенням).
10. Основна теорема арифметики (з доведенням). Канонічний розклад числа.
11. Твердження про зв'язок канонічного розкладу числа з його дільниками і наслідки з неї (з доведенням).
12. Лема про НСД двох чисел і остачі (з доведенням).
13. Алгоритм Евкліда (з доведенням).
14. Теорема про обчислювальну трудомісткість алгоритму Евкліда (з доведенням).
15. Лінійні діофантові рівняння. Теорема про існування розв'язків лінійного діофантового рівняння (з доведенням).

16. Теорема про нескінченну кількість розв'язків лінійного діофантового рівняння (з доведенням).

17. Метод розв'язання лінійного діофантового рівняння.

18. Мультиплікативна функція. Суматорна функція. Теорема про зв'язок між мультиплікативною і суматорною функціями (з доведенням).

19. Теорема про зв'язок канонічного розкладу числа з суматорною функцією (з доведенням) і наслідок з неї.

20. Функції $[x]$ і $\{x\}$. Теорема про канонічний розклад $n!$ і наслідок з неї (з доведенням).

21. Функція Ойлера, теорема про її мультиплікативність (з доведенням).

22. Теорема про зв'язок функції Ойлера з канонічним розкладом (з доведенням).

23. Теорема про суматорну функцію функції Ойлера (з доведенням).

24. Функція Мебіуса і твердження про її мультиплікативність (з доведенням).

25. Твердження про зв'язок мультиплікативних функцій з функцією Мебіуса (з доведенням).

26. Формула обертання Мебіуса (з доведенням).

27. Позиційна система числення, її побудова. Теорема про єдиність представлення числа (з доведенням).

28. Арифметичні дії в позиційних системах числення. Перехід між позиційними системами.

29. Ознаки подільності (з доведенням).

30. Систематичні дроби: скінченні і нескінченні. Теорма про зображення дробового числа (з доведенням).

31. Періодичні дроби. Передперіод, довжина передперіоду, період, довжина періоду.

32. Теорема про раціональні числа (з доведенням) і наслідок з неї.

33. Теорема про зображення нескоротного дробу.

1. Теорема про ділення з остачею

Теорема 1.1 (про ділення з остачею). *Для кожної пари цілих чисел a і b, $b \neq 0$, можна знайти такі цілі числа q і r, що*

$$a = qb + r \quad і \quad 0 \leq r < |b|. \tag{1.1}$$

Числа q і r цими умовами визначаються однозначно.

Знайдіть норм запис доведення будь ласка - так в книжці зрозуміле сука вітя а розписать його адекватно як

Доведення. Спочатку доведемо існування чисел q і r. Якщо $a = 0$, то можна взяти $q = r = 0$. Тому далі вважатимемо, що $a \neq 0$. Найперше розглянемо випадок, коли $a > 0$ і $b > 0$. Позначимо через A множину $A = \{a - nb \mid n \in \mathbb{Z}\}$. Серед її елементів є додатні числа (таким буде, наприклад, число $a-(-1)b = a+b$). Тому, згідно з принципом найменшого числа, серед невід'ємних чисел із множини A є найменше. Позначимо його через r і нехай $r = a - qb$ – зображення r як елемента множини A. Легко бачити, що $r < b$, бо в противному разі множина A містила б невід'ємне число $r - b = a - (q+1)b$, яке менше від r. Оскільки $r \geq 0$ і $a = qb + r$, то числа q і r – шукані.

Інші випадки легко зводяться до розглянутого. Справді, нехай числа p і s задовольняють умови $|a| = p \cdot |b| + s$ і $0 \leq s < |b|$. Якщо $s = 0$, то можна взяти $q = p \cdot \frac{ab}{|ab|}$ і $r = 0$. Якщо ж $s \neq 0$, то у випадку $a > 0$, $b < 0$ шуканими є числа $q = -p$, $r = s$, у випадку $a < 0$, $b > 0$ – числа $q = -p - 1$, $r = b - s$, а у випадку $a < 0$, $b < 0$ – числа $q = p + 1$ і $r = -b - s$.

Для доведення однозначності чисел q і r припустимо, що пара $(q_1; r_1)$ також задовольняє умовам $a = q_1 b + r_1$ і $0 \leq r_1 < |b|$. Тоді із $q_1 b + r_1 = qb + r$ випливає $|q_1 - q| \cdot |b| = |r - r_1|$. Очевидно, що $|r - r_1| < |b|$, бо числа r і r_1 лежать в інтервалі $[0, |b|)$. Звідси $|q_1 - q| \cdot |b| < |b|$ і $|q_1 - 1| < 1$. Оскільки число $q_1 - q$ – ціле, то $|q_1 - q| = 0$ і $q_1 = q$. Але тоді $r_1 = (q - q_1)b + r = r$, що й треба було довести. □

2.

Теорема 1.2 (про найпростіші властивості відношення подільності)**.**

(a) $a|a$ *(рефлексивність відношення подільності);*

(b) якщо $a|b$ *і* $b|c$*, то* $a|c$ *(транзитивність відношення подільності);*

(c) якщо $a|b$*, то* $a|bc$*;*

(d) якщо $a|b$ *і* $a|c$*, то* $a|(b \pm c)$*;*

(e) 0 *ділиться на кожне число, і немає інших чисел з такою властивістю;*

(f) кожне число ділиться на ± 1*, і немає інших чисел з такою властивістю;*

(g) якщо $a|b$ *і* $c|d$*, то* $ac|bd$*.*

В підручнику доведення нема - ну очев - ну іді нахуй - так ріл очев, чо піздєть

3.

Власні та невласні дільники, прості та складені числа, твердження про подільність кожного цілого числа на деяке просте число

До дільників числа a завжди належать числа ± 1 і $\pm a$. Такі дільники числа a називаються *невласними*, а всі інші – *власними*. Зауважимо, що дільник b числа $a \neq 0$ буде власним тоді й лише тоді, коли він задовольняє нерівності $1 < |b| < |a|$.

Число, яке має власні дільники, називається *складеним*. Якщо число не є складеним і відмінне від ± 1, то воно називається *простим*. Причина, чому числа ± 1 не відносять ні до простих, ні до складених, стане зрозумілою дещо пізніше. Очевидно, що відмінне від ± 1 число p буде простим тоді й лише тоді, коли для будь-якого розкладу p у добуток двох множників $p = ab$ один із них дорівнює ± 1.

Твердження 1.1. *Кожне відмінне від* ± 1 *ціле число ділиться на деяке просте число.*

Доведення. Скористаємось індукцією за модулем числа n. Для чисел 0 і ± 2 твердження очевидне. Розглянемо довільне n, $|n| > 2$, і припустимо, що для всіх чисел, модуль яких менший від $|n|$, твердження вже доведене. Якщо n – просте, то простим дільником числа n буде воно саме. Якщо ж n – складене, то воно має власний натуральний дільник m. Оскільки $1 < m < |n|$, то, за припущенням індукції, m має простий дільник p. Із транзитивності відношення подільності тепер випливає, що $p|n$. □

Теорема 1.3. *Кожне натуральне число розкладається в добуток простих чисел.*

Доведення. Для числа 1 твердження теореми випливає з нашої домовленості. Розглянемо тепер довільне $n > 1$ і припустимо, що для всіх чисел, менших від n, теорему вже доведено. Якщо n – просте, то шуканий

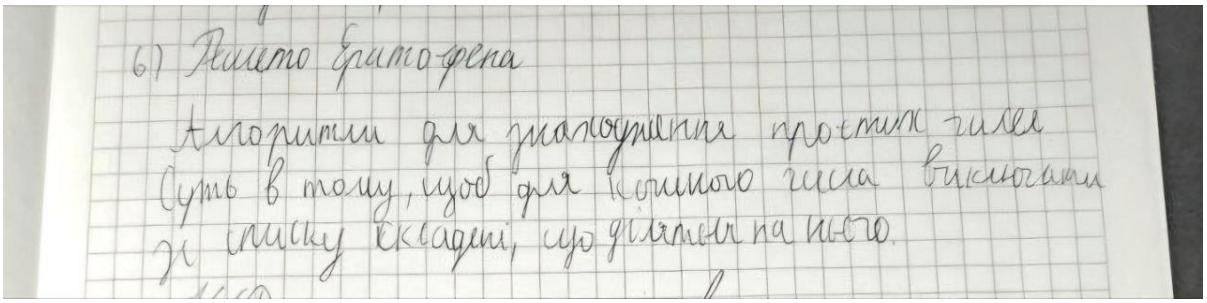
4.

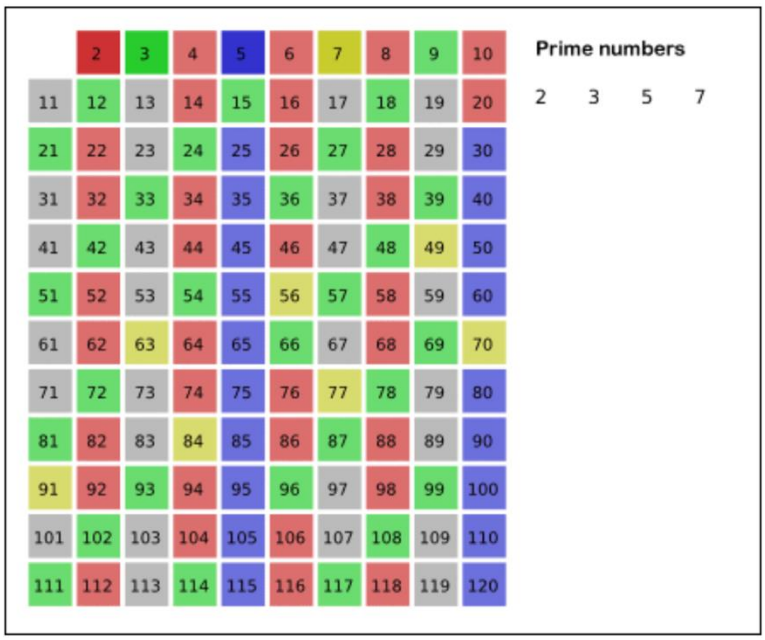
розклад для n складається з одного множника n. Якщо ж n складене, то за попереднім твердженням n можна розкласти в добуток $n = p_1 m$, де p_1 – просте і $m < n$. За припущенням індукції для m є розклад $m = p_2 p_3 \dots p_k$ у добуток простих чисел. Тоді $n = p_1 p_2 \dots p_k$ буде шуканим розкладом для числа n. □

Теорема 1.4 (Евклід)**.** *Існує нескінченно багато простих чисел.*

Доведення цієї теореми є класичним зразком доведення від супротивного. Справді, припустимо, що множина простих чисел скінченна, і нехай $p_1, p_2, \dots, p_k$ – їх повний список. Розглянемо число $n = p_1 p_2 \cdots p_k + 1$. За доведеним твердженням n має простий дільник p. Цей дільник не може збігатися з жодним із чисел $p_1, \dots, p_k$, бо n на ці числа не ділиться. Отже, просте число p не зустрічається в списку $p_1, \dots, p_k$, що суперечить припущенню про його повноту. Теорему доведено. □

5.

6. 



	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

7. НСД і теорема про його існування з доведенням і наслідком
   Число d називають найбільшим спільним дільником чисел a і b, якщо воно задовольняє 2 умови:

   (a) $d|a$ *і* $d|b$;

   (b) якщо $c|a$ *і* $c|b$, *то* $c|d$.

   Найбільший спільний дільник чисел a і b позначають НСД(a, b) або (a, b).

Теорема 1.5 (про існування найбільшого спільного дільника)**.** *Для будь-яких цілих чисел a і b існує їх найбільший спільний дільник (a, b).*

Доведення. Безпосередньо перевіряється, що $0 = (0, 0)$. Тому далі можна вважати, що серед чисел a і b є ненульове. Розглянемо множину $I = \{ma + nb : m, n \in \mathbb{Z}\}$. Вона, зокрема, містить числа $a = 1 \cdot a + 0 \cdot b$, $b = 0 \cdot a + 1 \cdot b$, і разом із числом $ma + nb$ містить протилежне число $(-m)a + (-n)b$. Тому серед елементів множини I є натуральні числа. Позначимо через d найменше з них і доведемо, що d є найбільшим спільним дільником чисел a і b. Справді, нехай $d = m_0a + n_0b$. Припустимо, що a не ділить b. Тоді розділимо a на d з остачею: $a = qd + r$, $0 < r < d$, і матимемо: $r = a - qd = (1 - qm_0)a + (-qn_0)b \in I$, що суперечить вибору числа d.

Аналогічно доводиться, що $d|b$. Отже, першу умову з означення найбільшого спільного дільника число d задовольняє.

Припустимо тепер, що $c|a$ і $c|b$. Тоді існують розклади $a = ca_0$ і $b = cb_0$, звідки $d = m_0 \cdot ca_0 + n_0 \cdot cb_0 = c(m_0a_0 + n_0b_0)$. Таким чином, $c|d$. □

Наслідок 1. *Якщо $d = НСД(a, b)$, то можна підібрати такі цілі числа m і n, що $d = ma + nb$.*

8.

Теорема 1.6 (критерій взаємної простоти двох чисел)**.** *Числа a і b взаємно прості тоді й лише тоді, коли можна підібрати такі цілі числа m і n, що $ma + nb = 1$.*

Доведення. Необхідність умови випливає з наслідку 1 теореми 1.5, а достатність – із того, що будь-який спільний дільник чисел a і b буде і дільником суми $ma + nb$. Тому коли $ma + nb = 1$, то a і b не мають відмінних від 1 спільних дільників. □

Твердження 1.2. *(a) Якщо* $(a,b)=1$ *і* $(a,c)=1$, *то* $(a,bc)=1$.

(b) Якщо $a|bc$ *і* $(a,b)=1$, *то* $a|c$.

(c) Якщо $a|c$, $b|c$ *і* $(a,b)=1$, *то* $ab|c$.

Доведення. (a) За критерієм взаємної простоти чисел умови $(a,b)=1$ і $(a,c)=1$ рівносильні існуванню таких цілих чисел m, n, k, l, що $ma+nb=1$, $ka+lc=1$. Перемноживши ці рівності, одержимо: $(mka+mlc+nkb)\cdot c+nl\cdot bc=1$. За тим же критерієм звідси випливає, що $(a,bc)=1$.

(b) Помноживши обидві частини рівності $ma+nb=1$ на c, одержимо: $mac+nbc=c$. Оскільки $a|mac$ і $a|nbc$, то $a|c$.

(c) За умовою існують такі a_0, b_0, m і n, що $c=aa_0=bb_0$ і $ma+nb=1$. Тоді $c=mac+nbc=ma\cdot bb_0+nb\cdot aa_0=(mb_0+na_0)ab$. Отже, $ab|c$. □

Твердження 1.3. *Якщо* $(a,b)=d$ *і* $a=a_0d$, $b=b_0d$, *то числа* a_0 *і* b_0 *взаємно прості.*

Доведення. Зобразимо d у вигляді $d=ma+nb=ma_0d+nb_0d$. Тоді після скорочення на d матимемо: $1=ma_0+nb_0$. Отже, за критерієм взаємної простоти чисел, $(a_0,b_0)=1$. □

9.

Число m називається *найменшим спільним кратним* чисел a і b, якщо воно задовольняє дві умови:

(a) $a|m$ *і* $b|m$;

(b) якщо $a|n$ *і* $b|n$, *то* $m|n$.

Найменше спільне кратне чисел a і b позначають НСК(a,b) або $[a,b]$.

Теорема про зв'язок нск і нсд

Теорема 1.7. *Для натуральних чисел* a *і* b $[a,b]=\frac{ab}{(a,b)}$.

Доведення. Нехай $(a,b)=d$. Тоді $a=a_0d$, $b=b_0d$ і $\frac{ab}{(a,b)}=a_0b_0d$. Очевидно, що $m=a_0b_0d=b_0a=a_0b$ є спільним кратним чисел a і b. Нехай тепер M – якесь спільне кратне чисел a і b. Тоді $M=aa_1=bb_1$. За твердженням 1.3 $(a_0,b_0)=1$, а тому існують такі числа k і l, що $1=ka_0+lb_0$. Помножимо обидві частини цієї рівності на M, матимемо: $M=ka_0M+lb_0M=ka_0bb_1+lb_0aa_1=kmb_1+lma_1=m(kb_1+la_1)$. Отже, $m|M$. □

10.

Теорема 1.8 (основна теорема арифметики)**.** *Кожне натуральне число розкладається в добуток простих чисел, причому такий розклад є однозначним з точністю до порядку і знаків множників.*

Доведення. Існування розкладу вже доведене (теорема 1.3), тому обгрунтування вимагає лише однозначність розкладу. Скористаємось індукцією за довжиною k найкоротшого розкладу числа (тобто розкладу, який містить найменшу кількість простих множників). Якщо $k = 0$ (число 1) або $k = 1$ (прості числа), то однозначність розкладу очевидна.

Нехай для всіх чисел, для яких існує розклад на менше ніж k простих множників, однозначність розкладу вже доведена, і нехай

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m \quad (m \geq k) \tag{1.2}$$

– два розклади числа n на прості множники. Якщо $(p_1, q_1) = 1$, $(p_1, q_2) = 1, \ldots, (p_1, q_m) = 1$, то з твердження 1.2$(a)$ випливає, що $(p_1, q_1 q_2 \cdots q_m) = 1$. Але це суперечить рівності (1.2). Тому існує таке i, що $(p_1, q_i) \neq 1$. Оскільки p_1 і q_i – прості числа, то вони відрізняються щонайбільше знаком. Змінивши, у разі потреби, в добутку $q_1 q_2 \cdots q_m$ порядок множників і знаки двох множників, можемо вважати, що $i = 1$ та $p_1 = q_1$. Тоді рівність (1.2) набуває вигляду $p_1 p_2 \ldots p_k = p_1 q_2 \ldots q_m$. Після скорочення на p_1 отримаємо: $p_2 \cdots p_k = q_2 \cdots q_m$. Але добуток у лівій частині цієї рівності містить уже менше, ніж k множників. Тому за припущенням

індукції кількість множників в обох частинах рівності однакова (тобто $k - 1 = m - 1$ і $k = m$), а добутки $p_2 \cdots p_k$ і $q_2 \cdots q_m$ розрізняються щонайбільше порядком і знаками множників. Якщо згадати, що $p_1 = q_1$, то однозначність розкладу числа n доведена. □

11.

Твердження 1.4. *Якщо канонічний розклад числа n має вигляд $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, то кожний натуральний дільник d числа n має вигляд*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}, \text{ де } 0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \ldots, 0 \le \beta_m \le \alpha_m.$$

Доведення випливає із простого зауваження, що коли $n = d \cdot f$ і канонічні розклади множників d і f мають вигляд

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}, \ f = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m},$$

то канонічний розклад числа n має вигляд $n = p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \cdots p_m^{\beta_m+\gamma_m}$. □

Наслідок 1. *Якщо для чисел a і b відомі їх канонічні розклади $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$, то*

$$НСД(a,b) = p_1^{min(\alpha_1,\beta_1)} p_2^{min(\alpha_2,\beta_2)} \cdots p_m^{min(\alpha_m,\beta_m)},$$

$$НСК(a,b) = p_1^{max(\alpha_1,\beta_1)} p_2^{max(\alpha_2,\beta_2)} \cdots p_m^{max(\alpha_m,\beta_m)}.$$

Наслідок 2. *Числа a і b є взаємно простими тоді і лише тоді, коли кожне просте число входить із додатним показником у канонічний розклад не більше ніж одного з чисел a і b.*

Доведення. Із наслідку 1 твердження 1.4 випливає, що числа

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \text{ і } b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

взаємно прості тоді й лише тоді, коли $min(\alpha_1,\beta_1) = min(\alpha_2,\beta_2) = \ldots = min(\alpha_m,\beta_m) = 0$. Останнє рівносильне тому, що в кожній парі показників α_i, β_i принаймні один із показників дорівнює 0. □

12.

Лема 1.1. *Якщо $a = qb + r$, то $(a,b) = (b,r)$.*

Доведення. Нехай $(a,b) = d_1$, $(b,r) = d_2$. Із рівності $a = qb + r$ випливає, що $d_2|a$. Крім того, $d_2|b$. Тому $d_2|d_1$. З іншого боку, $d_1|a$, а з рівності $r = a - qb$ маємо, що $d_1|r$. Тому $d_1|d_2$. Отже, d_1 і d_2 – асоційовані. Позаяк вони додатні, то $d_1 = d_2$. □

13.

Теорема 1.9. *Остання ненульова остача r_k з послідовності остач (1.5) є найбільшим спільним дільником чисел a і b.*

Доведення. Використовуючи лему і правило побудови послідовності (1.5), отримуємо ланцюжок рівностей $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{k-1}, r_k) = r_k$. □

14.

Теорема 1.10. *Обчислення за допомогою алгоритму Евкліда найбільшого спільного дільника чисел a і b, $a > b > 0$, вимагає менше ніж $2\log_2 a$ кроків.*

Доведення. Для зручності позначимо $r_{-1} = a$, $r_0 = b$ і нехай r_k – остання ненульова остача при обчисленні НСД(a, b). Покажемо, що в послідовності остач $(r_{-1}, r_0, r_1, r_2, \ldots, r_{k-1}, r_k)$ за будь-які два кроки остача зменшується принаймні вдвічі, точніше, що для всіх i $r_{i+2} < \frac{1}{2}r_i$. Справді, якщо $r_{i+1} \leq \frac{1}{2}r_i$, то це твердження одразу випливає з нерівності $r_{i+2} \leq r_{i+1}$. Якщо ж $r_{i+1} > \frac{1}{2}r_i$, то $r_i - r_{i+1} < r_i - \frac{1}{2}r_i = \frac{1}{2}r_i < r_{i+1}$. Але з рівності $r_i = r_{i+1} + (r_i - r_{i+1})$тепер випливає, що остача r_{i+2} від ділення r_i на r_{i+1} дорівнює $r_i - r_{i+1}$. Тому $r_{i+2} = r_i - r_{i+1} < \frac{1}{2}r_i$.

Нехай тепер $2m - 1$ – найбільше непарне число, яке не перевищує k. Тоді $k \leq 2m$. Крім того, з нерівності $r_{i+2} < \frac{1}{2}r_i$ випливає, що $r_{2m-1} < \frac{a}{2^m}$.

Оскільки $r_{2m-1} \geq 1$, то $2^m < a$, звідки $m < \log_2 a$. Отже, $k \leq 2m < 2\log_2 a$, що й треба було довести. □

Теорема 1.11. *Лінійне діофантове рівняння $ax + by = c$ має розв'язки тоді й лише тоді, коли його права частина c ділиться на найбільший спільний дільник чисел a і b.*

Доведення. Необхідність умови очевидна, бо сума $ax + by$ завжди ділиться на найбільший спільний дільник d чисел a і b.

Достатність. Нехай $c = c_0 d$. За наслідком 1 теореми 1.5 існують такі цілі числа m і n, що $ma + nb = d$. Тоді з рівності $mc_0 a + nc_0 b = c_0 d$ випливає, що цілі числа $x = mc_0$ і $y = nc_0$ є розв'язком рівняння $ax + by = c$. □

Теорема 1.12. *Якщо лінійне діофантове рівняння*

$$ax + by = c \tag{1.6}$$

має цілий розв'язок x_0, y_0, то воно має нескінченно багато цілих розв'язків, і всіх їх можна знайти за формулами

$$x = x_0 - \frac{b}{d}k,\ y = y_0 + \frac{a}{d}k, \tag{1.7}$$

де d =НСД(a, b), a k – довільне ціле число.

Доведення. За умовою

$$ax_0 + by_0 = c. \tag{1.8}$$

Тому $a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ba}{d}k = ax_0 + by_0 = c$. Крім того, числа $\frac{b}{d}k$ і $\frac{a}{d}k$ – цілі. Отже, формули (1.7) справді визначають розв'язок рівняння (1.6).

Нехай тепер x, y – довільний розв'язок рівняння (1.6). Позначимо $\frac{a}{d} = a_0$, $\frac{b}{d} = b_0$. Віднімаючи (1.6) від рівності (1.8), одержимо $a(x_0 - x) + b(y_0 - y) = 0$ або, після ділення на d,

$$a_0(x_0 - x) + b_0(y_0 - y) = 0. \tag{1.9}$$

Звідси випливає, що $a_0 | b_0(y - y_0)$. Оскільки, за твердженням 1.2, числа a_0 і b_0 взаємно прості, то $a_0 | y - y_0$. Тому існує таке ціле число k, що $y - y_0 = a_0 k$ і $y = y_0 + a_0 k$. Рівність (1.9) тепер набуває вигляду $a_0(x_0 - x) = b_0 a_0 k$, звідки $x_0 - x = b_0 k$ і $x = x_0 - b_0 k$. Таким чином, кожен розв'язок рівняння (1.6) має вигляд (1.7), що й треба було довести. □

17.

(a) за допомогою алгоритму Евкліда знаходимо найбільший спільний дільник $d = (a, b)$ і перевіряємо, чи $d|c$. Якщо $d \nmid c$, то рівняння розв'язків не має.

(b) Якщо $d|c$, то за допомогою алгоритму Евкліда знаходимо зображення $d = ma + nb$ і частковий розв'язок $x_0 = m\frac{c}{d}$, $y_0 = n\frac{c}{d}$.

(c) Знаходимо загальний розв'язок

$$x = m\frac{c}{d} - \frac{b}{d}k,\ y = n\frac{c}{d} + \frac{a}{d}k,\ k \in \mathbb{Z}.$$

18.

Функція $f(n)$, що визначена на множині всіх натуральних чисел і набуває дійсних значень, називається *мультиплікативною*, якщо виконуються такі умови:

(a) функція $f(n)$ не є тотожно рівною нулю;

(b) для довільних взаємно простих натуральних чисел m і n виконується рівність $f(mn) = f(m)f(n)$.

19.

Наступна конструкція дозволяє будувати нові мультиплікативні функції. Для довільної визначеної на множині натуральних чисел функції $f(n)$ розглянемо функцію $F(n) = \sum\limits_{d|n} f(d)$ (тобто сума береться по всім натуральним дільникам d числа n), яка називається *суматорною* функцією для функції $f(n)$.

Отже, суматорна функція $F(n)$ є мультиплікативною.

Достатність. Нехай функція $F(n)$ – мультиплікативна. Тоді $f(1) = F(1) = 1$. Очевидно, що $f(1 \cdot 1) = f(1) = 1 = 1 \cdot 1 = f(1) \cdot f(1)$. Нехай тепер m і n – довільні взаємно прості числа. Припустимо, що для всіх взаємно простих чисел l і t, таких, що $lt < mn$, рівність $f(lt) = f(l)f(t)$ уже доведена, і покажемо, що $f(mn) = f(m)f(n)$. Справді,

$$\sum_{l|m}\sum_{t|n} f(lt) = F(mn) = F(m)F(n) = \sum_{l|m} f(l) \sum_{t|n} f(t). \qquad (2.1)$$

Розпишемо ліву і праву суми таким чином:

$$\sum_{l|m}\sum_{t|n} f(lt) = \sum_{\substack{l|m\\ l\neq m}} f(lt) + \sum_{t|n} f(mt) = \sum_{\substack{l|m\\ l\neq m}} f(lt) + \sum_{\substack{t|n\\ t\neq n}} f(mt) + f(mn),$$

$$\sum_{l|m} f(l) \sum_{t|n} f(t) = \sum_{l|m}\sum_{t|n} f(l)f(t) = \sum_{\substack{l|m\\ l\neq m}} f(l)f(t) + \sum_{\substack{t|n\\ t\neq n}} f(m)f(t) + f(m)f(n).$$

За припущенням $f(lt) = f(l)f(t)$, поки $lt < mn$. Тому

$$\sum_{\substack{l|m\\ l\neq m}} f(lt) = \sum_{\substack{l|m\\ l\neq m}} f(l)f(t) \text{ і } \sum_{\substack{t|n\\ t\neq n}} f(mt) = \sum_{\substack{t|n\\ t\neq n}} f(m)f(t).$$

Із рівності (2.1) тепер випливає $f(mn) = f(m)f(n)$, що й вимагалось. □

Теорема 2.2. *Нехай $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ – канонічний розклад числа n. Тоді для мультиплікативної функції $f(n)$ її суматорна функція $F(n)$ дорівнює*

$$F(n) = (1 + f(p_1) + f(p_1^2) + f(p_1^{\alpha_1})) \cdots (1 + f(p_k) + f(p_k^2) + f(p_k^{\alpha_k})). \quad (2.2)$$

Доведення. Після розкриття дужок у правій частині рівності (2.2) отримаємо суму доданків вигляду $f(p_1^{\beta_1}) \cdots f(p_k^{\beta_k}) = f(p_1^{\beta_1} \cdots p_k^{\beta_k})$, де $0 \leq \beta_1 \leq \alpha_1, \ldots, 0 \leq \beta_k \leq \alpha_k$, причому для кожного можливого набору $(\beta_1, \ldots, \beta_k)$ буде зустрічатись рівно один доданок. Але коли набір $(\beta_1, \ldots, \beta_k)$ пробігає всі можливі значення, то добуток $p_1^{\beta_1} \cdots p_k^{\beta_k}$ пробігає всі можливі дільники числа n, тому права частина рівності (2.2) дорівнює $F(n)$. □

20.

Теорема 2.3. *Степінь l, в якому просте число p входить до канонічного розкладу числа $n!$, дорівнює $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$.*

Доведення. Зауважимо, що $\left[\frac{n}{p}\right]$ дорівнює кількості тих чисел ряду 1, 2, …, n, які діляться на p, $\left[\frac{n}{p^2}\right]$ – кількості тих чисел цього ряду, які діляться на p^2, і т.д. Тому, міняючи порядок сумування, одержуємо:

$$l = \sum_{m=1}^{n} \sum_{\substack{j=1 \\ p^j | m}}^{\infty} 1 = \sum_{j=1}^{\infty} \sum_{\substack{m=1 \\ p^j | m}}^{n} 1 = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right],$$

що й вимагалось довести. □

22.

Для натурального числа n *функція Ойлера* $\varphi(n)$ визначається як кількість чисел ряду $1, 2, \ldots, n$, які взаємно прості з числом n. Так, $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$.

(Доведення мультиплікативності в книзі (це пізда воно велике))

23.

Теорема 2.6. *Нехай* $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ *— канонічний розклад числа* n*. Тоді*

$$\varphi(n) = n\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots\Big(1-\frac{1}{p_k}\Big) = (p_1-1)\cdots(p_k-1)p_1^{\alpha_1-1}\cdots p_k^{\alpha_k-1}\,. \tag{2.11}$$

Зокрема, для простого числа p $\quad \varphi(p) = p-1$ *і* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Доведення. Розглянемо спочатку випадок $n = p^\alpha$, де p — просте число. Зрозуміло, що число m буде взаємно простим із числом p^α тоді й лише тоді, коли m не ділиться на p. Серед чисел $1, \ldots, p, p+1, \ldots, 2p, 2p+1, \ldots, p^2, p^2+1, \ldots, p^2+p, p^2+p+1, \ldots, 2p^2, 2p^2+1, \ldots, p^\alpha$ на p будуть ділитися числа $p, 2p, \ldots, p^2, p^2+p, \ldots, p^\alpha$, тобто кожне p–те число. Тому таких чисел буде $p^\alpha/p = p^{\alpha-1}$. Решта $p^\alpha - p^{\alpha-1}$ чисел взаємно прості з p, а отже, і з p^α. Тому $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Зокрема, $\varphi(p) = p^1 - p^0 = p-1$.

Використовуючи мультиплікативність функції φ (теорема 2.5), у загальному випадку маємо:

$$\varphi\Big(p_1^{\alpha_1}\cdots p_k^{\alpha_k}\Big) = \varphi\Big(p_1^{\alpha_1}\Big)\cdots\varphi\Big(p_k^{\alpha_k}\Big) = \Big(p_1^{\alpha_1} - p_1^{\alpha_1-1}\Big)\cdots\Big(p_k^{\alpha_k} - p_k^{\alpha_k-1}\Big) =$$
$$p_1^{\alpha_1}\Big(1-\tfrac{1}{p_1}\Big)\cdots p_k^{\alpha_k}\Big(1-\tfrac{1}{p_k}\Big) = n\Big(1-\tfrac{1}{p_1}\Big)\cdots\Big(1-\tfrac{1}{p_k}\Big),$$

що й треба було довести. □

24.

Твердження 2.1. *Для кожного натурального числа* n

$$\sum_{d|n}\varphi(d) = n\,.$$

Доведення. Функція $F(n) = \sum\limits_{d|n}\varphi(d)$ є суматорною для функції $\varphi(n)$. Нехай $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ – канонічний розклад числа n. Позаяк $\varphi(n)$ мультиплікативна, то за теоремою 2.2 маємо: $F(n) = \Big(1+\varphi\big(p_1\big)+\varphi\big(p_1^2\big)+\cdots+\varphi\big(p_1^{\alpha_1}\big)\Big)\cdots\Big(1+\varphi\big(p_k\big)+\varphi\big(p_k^2\big)+\cdots+\varphi\big(p_k^{\alpha_k}\big)\Big)$. Але за теоремою 2.6 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Тому $F(n) = \Big(1+(p_1-1)+\big(p_1^2-p_1\big)+\cdots+\big(p_1^{\alpha_1}-p_1^{\alpha_1-1}\big)\Big)\cdots$
$\cdots\Big(1+(p_k-1)+\big(p_k^2-p_k\big)+\cdots+\big(p_k^{\alpha_k}-p_k^{\alpha_k-1}\big)\Big) = p_1^{\alpha_1}\cdots p_k^{\alpha_k} = n$, що й вимагалось. □

2.4. Функція Мебіуса $\mu(n)$

Функція Мебіуса $\mu(n)$ визначається на множині натуральних чисел такими умовами: $\mu(1) = 1$; $\mu(n) = (-1)^s$, якщо канонічний розклад числа n має вигляд $n = p_1 \cdots p_s$, і $\mu(n) = 0$, якщо в канонічному розкладі $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ числа n хоча б один із показників $\alpha_1, \ldots, \alpha_k$ більший за 1 (тобто якщо n ділиться на квадрат хоча б одного простого числа).

Твердження 2.2. *Функція Мебіуса* $\mu(n)$ *і її суматорна функція* $\nu(n) = \sum_{d|n} \mu(d)$ *— мультиплікативні.*

Доведення. Перша частина твердження випливає безпосередньо з означення функції $\mu(n)$, а друга — з теореми 2.1 . □

25.

Твердження 2.3. *Нехай $f(n)$ — мультиплікативна функція, а $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ — канонічний розклад числа n. Тоді*

$$\sum_{d|n} \mu(d) f(d) = \big(1 - f(p_1)\big) \cdots \big(1 - f(p_k)\big)$$

(як завжди, добуток нульової кількості множників вважається рівним 1, тому для $n = 1$ права частина рівності дорівнює 1). Зокрема, для функції $f(n) = 1$ маємо

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{якщо } n = 1, \\ 0, & \text{якщо } n > 1, \end{cases} \tag{2.14}$$

а для функції $f(n) = 1/n$ —

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases} 1, & \text{якщо } n = 1, \\ \left(1 - \dfrac{1}{p_1}\right) \cdots \left(1 - \dfrac{1}{p_k}\right), & \text{якщо } n > 1. \end{cases} \tag{2.15}$$

Доведення. Функція $\theta(n) = \mu(n) f(n)$ є мультиплікативною як добуток мультиплікативних функцій $\mu(n)$ і $f(n)$. А тому, за теоремою 2.2,

$$\sum_{d|n} \theta(d) = \big(1 + \theta(p_1) + \cdots + \theta(p_1^{\alpha_1})\big) \cdots \big(1 + \theta(p_k) + \cdots + \theta(p_k^{\alpha_k})\big) \,,$$

де $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ — канонічний розклад числа n. Враховуючи, що $\theta(p_i) = \mu(p_i) f(p_i) = -f(p_i)$ і $\theta(p_i^j) = 0$ для $j > 1$, переконуємося в справедливості твердження. □

26.

Теорема 2.7. *Нехай $f(n)$ — довільна функція, визначена на множині натуральних чисел, а $g(n) = \sum_{d|n} f(d)$ — її суматорна функція. Тоді*

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right). \tag{2.16}$$

Доведення. Справді,

$$\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \left(\mu(d) \sum_{t|(n/d)} f(t)\right) = \sum_{t|n} \left(f(t) \sum_{d|(n/t)} \mu(d)\right). \tag{2.17}$$

Але з рівності (2.14) випливає, що коли $t \neq n$, то $\sum_{d|(n/t)} \mu(d) = 0$. Тому в правій частині рівності (2.17) лишається лише один доданок $f(n) \sum_{d|(n/n)} \mu(d) = f(n)\mu(1) = f(n)$, що й вимагалось. □

27.

$$n = r_k m^k + r_{k-1} m^{k-1} + \cdots + r_1 m + r_0,$$

Теорема 3.1. *Нехай натуральне число $m > 1$ – фіксоване. Тоді кожне натуральне число n єдиним чином зображується в позиційній системі числення з основою m.*

Доведення. Існування зображення доведено вище. Для доведення єдиності розглянемо два зображення числа n в m-ковій системі: $n = r_k m^k + \cdots + r_0$ і $n = s_l m^l + \cdots + s_0$. Якщо від першого зображення відняти друге, одержимо рівність

$$0 = (r_0 - s_0) + (r_1 - s_1)m + (r_2 - s_2)m^2 + \cdots. \tag{3.2}$$

Зауважимо, що $r_i \geq r_i - s_i \geq -s_i$, тому $|r_i - s_i| \leq m - 1$ для всіх i. Припустимо, що серед коефіцієнтів $r_0 - s_0$, $r_1 - s_1$, ... є ненульові. Нехай $r_j - s_j$ – останній з них. Тоді рівності (3.2) можна надати вигляду

$$(r_0 - s_0) + \ldots + (r_{j-1} - s_{j-1})m^{j-1} = (s_j - r_j)m^j, \tag{3.3}$$

де права частина задовольняє нерівність $|(s_j - r_j)m^j| = |s_j - r_j| \cdot m^j \geq m^j$, а ліва – нерівності $|(r_0 - s_0) + (r_1 - s_1)m + \cdots + (r_{j-1} - s_{j-1})m^{j-1}| \leq |(r_0 - s_0)| + |r_1 - s_1|m + \cdots + |r_{j-1} - s_{j-1}|m^{j-1} \leq (m-1) + (m-1)m + \cdots + (m-1)m^{j-1} = (m-1)(1 + m + \cdots + m^{j-1}) = m^j - 1 \leq m^j$. Оскільки нерівності для лівої і правої частин (3.3) суперечать одна одній, то припущення про наявність в (3.2) ненульового коефіцієнта є хибним. Тому $r_0 - s_0 = 0, r_1 - s_1 = 0, \ldots$, звідки $r_0 = s_0, r_1 = s_1, \ldots$, що й доводить єдиність зображення числа n. □

Щоб побудувати *позиційну систему числення*, зафіксуємо натуральне число $m > 1$ (*основу системи*). Візьмемо довільне натуральне число n і почнемо ділити його на m з остачею, аж поки частка не стане рівною 0 (таке рано чи пізно трапиться, бо кожного разу частка зменшуватиметься):

$$n = q_1 m + r_0,\ 0 \le r_0 < m, \qquad q_1 = q_2 m + r_1,\ 0 \le r_1 < m$$

$$q_2 = q_3 m + r_2,\ 0 \le r_2 < m, \qquad \dots,$$

$$q_{k-1} = q_k m + r_{k-1},\ 0 \le r_{k-1} < m, \qquad q_k = 0 \cdot m + r_k,\ 0 \le r_k < m.$$

Цей ланцюжок рівностей можна "розкрутити" наступним чином: $n = q_1 m + r_0 = (q_2 m + r_1)m + r_0 = q_2 m^2 + r_1 m + r_0 = (q_3 m + r_2)m^2 + r_1 m + r_0 =$

$q_3 m^3 + r_2 m^2 + r_1 m + r_0 = \dots = q_k m^k + r_{k-1} m^{k-1} + \dots + r_1 m + r_0 = r_k m^k + r_{k-1} m^{k-1} + \dots + r_1 m + r_0$. Одержана рівність

$$n = r_k m^k + r_{k-1} m^{k-1} + \dots + r_1 m + r_0, \tag{3.1}$$

де $r_k \ne 0$ і $0 \le r_j < m$ для всіх $j = 0, 1, \dots, k$, називається *зображенням числа n у позиційній системі числення з основою m* (або в *m-ковій позиційній системі числення* чи просто в *m-ковій системі*).

Теорема 3.1. *Нехай натуральне число $m > 1$ – фіксоване. Тоді кожне натуральне число n єдиним чином зображується в позиційній системі числення з основою m.*

Доведення. Існування зображення доведено вище. Для доведення єдиності розглянемо два зображення числа n в m-ковій системі: $n = r_k m^k + \dots + r_0$ і $n = s_l m^l + \dots + s_0$. Якщо від першого зображення відняти друге, одержимо рівність

$$0 = (r_0 - s_0) + (r_1 - s_1)m + (r_2 - s_2)m^2 + \dots . \tag{3.2}$$

Зауважимо, що $r_i \geq r_i - s_i \geq -s_i$, тому $|r_i - s_i| \leq m - 1$ для всіх i. Припустимо, що серед коефіцієнтів $r_0 - s_0, r_1 - s_1, \dots$ є ненульові. Нехай $r_j - s_j$ – останній з них. Тоді рівності (3.2) можна надати вигляду

$$(r_0 - s_0) + \dots + (r_{j-1} - s_{j-1})m^{j-1} = (s_j - r_j)m^j, \tag{3.3}$$

де права частина задовольняє нерівність $|(s_j - r_j)m^j| = |s_j - r_j| \cdot m^j \geq m^j$, а ліва – нерівності $|(r_0 - s_0) + (r_1 - s_1)m + \dots + (r_{j-1} - s_{j-1})m^{j-1}| \leq |(r_0 - s_0)| + |r_1 - s_1|m + \dots + |r_{j-1} - s_{j-1}|m^{j-1} \leq (m-1) + (m-1)m + \dots + (m-1)m^{j-1} = (m-1)(1 + m + \dots + m^{j-1}) = m^j - 1 \leq m^j$. Оскільки нерівності для лівої і правої частин (3.3) суперечать одна одній, то припущення про наявність в (3.2) ненульового коефіцієнта є хибним. Тому $r_0 - s_0 = 0, r_1 - s_1 = 0, \dots$, звідки $r_0 = s_0, r_1 = s_1, \dots$, що й доводить єдиність зображення числа n. □

3.2. Арифметичні дії в позиційних системах

Знайомі з дитинства правила виконання арифметичних дій над числами, записаними в десятковій системі, з очевидними невеликими змінами (інший набір цифр, інша таблиця множення) можна застосувати в будь-якій позиційній системі. Тому ми тільки проілюструємо ці правила прикладами.

(a) *Додавання.*

$$\begin{array}{r} 3\,3\,0\,1\,4\,3_5 \\ +\,\underline{3\,4\,2\,0\,2\,4_5} \\ 1\,2\,2\,2\,2\,2\,2_5 \end{array} \quad ; \quad \begin{array}{r} 3\,3\,0\,1\,4\,3_7 \\ +\,\underline{3\,4\,2\,0\,2\,4_7} \\ 1\,2\,2\,2\,2\,2\,2_7 \end{array} \quad ; \quad \begin{array}{r} 3\,3\,0\,1\,4\,3_8 \\ +\,\underline{3\,4\,2\,0\,2\,4_8} \\ 1\,2\,2\,2\,2\,2\,2_8 \end{array} \quad .$$

Незважаючи на позірну схожість доданків, суми вийшли дуже різними. Це й зрозуміло, адже одна й та ж послідовність символів у системах із різними основами позначає зовсім різні числа.

(b) *Віднімання.*

$$\begin{array}{r} 2\,2\,3\,1\,0\,3_5 \\ -\,\underline{1\,3\,2\,4\,1\,4_5} \\ 4\,0\,1\,3\,4_5 \end{array} \quad ; \quad \begin{array}{r} 2\,2\,3\,1\,0\,3_7 \\ -\,\underline{1\,3\,2\,4\,1\,4_7} \\ 6\,0\,3\,5\,6_7 \end{array} \quad ; \quad \begin{array}{r} 2\,2\,3\,1\,0\,3_8 \\ -\,\underline{1\,3\,2\,4\,1\,4_8} \\ 7\,0\,4\,6\,7_8 \end{array} \quad .$$

(c) *Множення "стовпчиком".* Як і в десятковій системі, в кожній позиційній системі для виконання множення зручно користуватись готовою таблицею множення одноцифрових чисел. Наведемо таку таблицю для сімкової системи. Щоб не захаращувати таблицю, ми скрізь опустимо нижній індекс 7, який вказує на основу системи

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	11	13	15
3	3	6	12	15	21	24
4	4	11	15	22	26	33
5	5	13	21	26	34	42
6	6	15	24	33	42	51

(e) Особливо простого вигляду набувають таблиці *додавання і множення одноцифрових чисел у двійковій системі числення:*

$+$	0	1
0	0	1
1	1	0

;

$\times$	0	1
0	0	0
1	0	1

.

Тому в цій системі особливо легко виконувати арифметичні дії:

$$\begin{array}{r} 1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1_2 \\ +\ 1\,0\,1\,1\,0\,0\,1\,1\,1\,0\,0\,1_2 \\ \hline 1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0_2 \end{array} \quad ; \quad \begin{array}{r} 1\,1\,1\,0\,1\,1\,0\,1_2 \\ \times\ 1\,0\,1\,1\,0\,1\,0\,1_2 \\ \hline 1\,1\,1\,0\,1\,1\,0\,1_2 \\ 1\,1\,1\,0\,1\,1\,0\,1_2 \\ 1\,1\,1\,0\,1\,1\,0\,1_2 \\ 1\,1\,1\,0\,1\,1\,0\,1_2 \\ 1\,1\,1\,0\,1\,1\,0\,1_2 \\ \hline 1\,0\,1\,0\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1_2 \end{array} .$$

$$\begin{array}{r} 2\,5\,1\,3_7 \\ \times\ 4\,6\,2\,5_7 \\ \hline 1\,6\,5\,0\,1_7 \\ 5\,3\,2\,6_7 \\ 2\,2\,3\,1\,4_7 \\ 1\,3\,6\,5\,5_7 \\ \hline 1\,6\,3\,2\,2\,4\,6\,1_7 \end{array} \quad ; \quad \begin{array}{r} 3\,0\,2\,1\,4_7 \\ \times\ 2\,6\,1\,0\,5_7 \\ \hline 2\,1\,1\,4\,0\,6_7 \\ 3\,0\,2\,1\,4_7 \\ 2\,4\,1\,6\,2\,3_7 \\ 6\,0\,4\,3\,1_7 \\ \hline 1\,1\,5\,2\,4\,6\,6\,1\,0\,6_7 \end{array} .$$

(d) *Ділення "ріжком".*

$$\begin{array}{r|l} 2\,3\,5\,3\,0\,4_7 & 1\,2\,3_7 \\ \cline{2-2} -\ 1\,2\,3_7 & 1\,6\,1\,2_7 \\ \cline{1-1} 1\,1\,2\,3_7 & \\ -\ 1\,1\,0\,4_7 & \\ \cline{1-1} 1\,6\,0_7 & \\ -\ 1\,2\,3_7 & \\ \cline{1-1} 3\,4\,4_7 & \\ -\ 2\,4\,6_7 & \\ \cline{1-1} 6\,5_7 & \end{array}$$

Таким чином, при діленні з остачею 235304_7 на 123_7 одержуємо частку 1612_7 й остачу 65_7, тобто $235304_7 = 123_7 \cdot 1612_7 + 65_7$.

3.3. Перехід до іншої позиційної системи

Може виникнути потреба перейти від запису числа $n = (a_k \dots a_2 a_1 a_0)_m$ в одній позиційній системі до його запису $n = (b_t \dots b_2 b_1 b_0)_p$ в іншій системі. Наприклад, від звичної для людини десяткової системи до зручної для машини двійкової. Є два основні способи здійснення такого переходу.

I спосіб грунтується на рівності $n = b_t p^t + b_{t-1} p^{t-1} + \dots + b_2 p^2 + b_1 p + b_0 = ((\dots((b_t p + b_{t-1})p + b_{t-2})p + \dots + b_2)p + b_1)p + b_0$. Виконуючи в m-ковій системі ділення з остачею числа на p, послідовно знаходимо:

$$\text{частку } (\dots((b_t p + b_{t-1})p + b_{t-2})p + \dots + b_2)p + b_1 \text{ й остачу } b_0;$$

$$\text{частку } \dots((b_t p + b_{t-1})p + b_{t-2})p + \dots + b_2 \text{ й остачу } b_1; \ \dots \ ;$$

$$\text{частку } b_t p + b_{t-1} \text{ й остачу } b_{t-2}; \ \text{частку } b_t \text{ й остачу } b_{t-1};$$

$$\text{частку } 0 \text{ й остачу } b_t.$$

Остачі b_t, b_{t-1}, b_{t-2}, …, b_1, b_0 є цифрами числа n у системі числення з основою p.

II спосіб використовує рівність

$$n = a_k m^k + a_{k-1} m^{k-1} + \dots + a_2 m^2 + a_1 m + a_0 = \\ = ((\dots((a_k m + a_{k-1})m + a_{k-2})m + \dots + a_2)m + a_1)m + a_0 \ . \qquad (3.4)$$

Записавши m і кожну з цифр a_k, a_{k-1}, …, a_1, a_0 у системі з основою p, обчислюємо n у цій же системі за формулою (3.4). Самі обчислення зручно організувати в таблицю (так звану *схему Горнера*), всі елементи якої обчислюються за одним і тим же правилом:

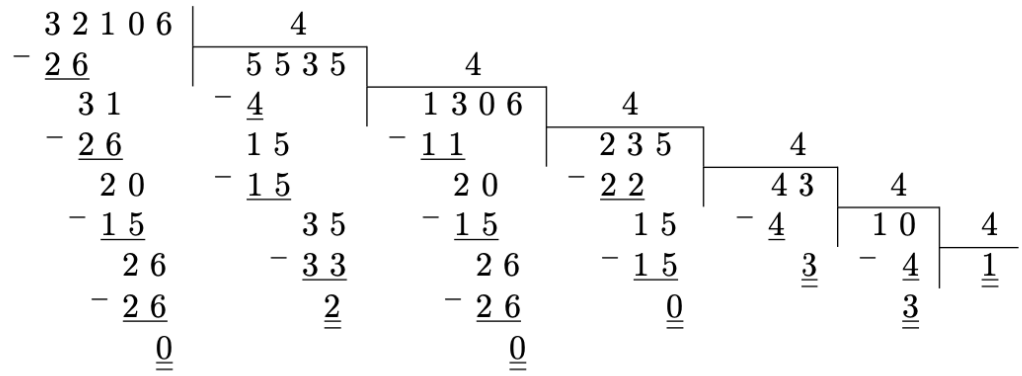
	a_k	a_{k-1}	a_{k-2}	…	a_1	a_0
m	$c_k =$	$c_{k-1} =$	$c_{k-2} =$	…	$c_1 =$	$c_0 =$
	a_k	$mc_k + a_{k-1}$	$mc_{k-1} + a_{k-2}$	…	$mc_2 + a_1$	$mc_1 + a_0$

Останній елемент c_0 збігається, як бачимо, з числом n.

Таким чином, способи розрізняються вибором системи, в якій проводяться обчислення: “старої” з основою m у першому способі і “нової” з основою p – у другому.

Задача 3.3. *Записати число* 32106_7 *в системі числення з основою* 4.

Розв'язання. I спосіб. Щоб не захаращувати записів, ми опускатимемо в обчисленнях нижній індекс 7, який вказує на основу системи.



Отже, $32106_7 = 1330020_4$.

II спосіб. Заміняємо число 7 і цифри числа 32106_7 їх записами в 4-ковій системі й далі всі обчислення проводимо в цій системі (нижній індекс 4, який вказує на основу системи, знову для зручності опускаємо).

	3	2	1	0	12
13	3	$3 \cdot 13 + 2$ $= 113$	$113 \cdot 13 + 1$ $= 2202$	$2202 \cdot 13 + 0$ $= 101232$	$101232 \cdot 13 + 12$ $= 1330020$

Отже, $32106_7 = 1330020_4$. □

Твердження 3.1. *Нехай d є дільником основи m. Число $n = (a_k \dots a_1 a_0)_m$ ділиться на d тоді й лише тоді, коли його остання цифра a_0 ділиться на d.*

Доведення. За умовою у правій частині рівності $n = a_k m^k + \dots + a_1 m + a_0$ всі доданки, крім останнього, діляться на d. Тому для подільності n на d необхідно й достатньо, щоб і останній доданок a_0 також ділився на d. □

Ця ознака є узагальненням ознак подільності на 2, 5 і 10 у десятковій системі числення. Її можна сформулювати у більш загальному вигляді.

Твердження 3.2. *Нехай для деякого натурального r число d є дільником числа m^r. Число $n = (a_k \dots a_1 a_0)_m$ ділиться на d тоді й лише тоді, коли на d ділиться число $(a_{r-1} \dots a_1 a_0)_m$, утворене останніми r цифрами числа n.*

Доведення. Рівність $n = a_k m^k + \dots + a_r m^r + a_{r-1} m^{r-1} + \dots + a_1 m + a_0$ можна переписати у вигляді: $n = a_k m^k + \dots + a_r m^r + (a_{r-1} \dots a_1 a_0)$ і повторити міркування з попереднього доведення. □

Твердження 3.3. *Нехай d є дільником числа $m - 1$. Число $n = (a_k \dots a_1 a_0)_m$ ділиться на d тоді й лише тоді, коли на d ділиться сума $a_k + \dots + a_1 + a_0$ його цифр.*

Доведення. Із рівності $m^r - 1 = (m-1)(m^{r-1} + m^{r-2} + \dots + m + 1)$ випливає, що кожне з чисел $m - 1$, $m^2 - 1$, …, $m^k - 1$ ділиться на d. Записуючи n у вигляді $n = a_k m^k + \dots + a_1 m + a_0 = a_k(m^k - 1) + \dots + a_1(m - 1) + (a_k + \dots + a_1 + a_0)$, бачимо, що всі доданки, крім останнього, напевне діляться на d. Тому для подільності n на d необхідно й достатньо, щоб і останній доданок $a_k + \dots + a_1 + a_0$ також ділився на d. □

Твердження 3.4. *Нехай d є дільником числа $m+1$. Число $n = (a_k \dots a_1 a_0)_m$ ділиться на d тоді й лише тоді, коли на d ділиться сума $a_0 - a_1 + a_2 - \dots + (-1)^k a_k$.*

Доведення. За допомогою індукції легко довести, що для кожного натурального r число m^r можна записати у вигляді $m^r = (-1)^r + A_r \cdot (m+1)$, де A_r – ціле число. Справді, для $r = 1$ і $r = 2$ це очевидно: $m^1 = (-1)^1 + 1 \cdot (m+1)$, $m^2 = (-1)^2 + (m-1) \cdot (m+1)$. Індукційний крок також перевіряється просто. Якщо $r > 2$, то $m^r = m^{r-2} \cdot m^2 = ((-1)^{r-2} + A_{r-2}(m+1)) \cdot ((-1)^2 + (m-1)(m+1)) = (-1)^r + ((-1)^{r-2}(m-1) + (-1)^2 A_{r-2} + A_{r-2}(m^2-1)) \cdot (m+1) = (-1)^r + A_r(m+1)$, де $A_r = (-1)^{r-2}(m-1) + (-1)^2 A_{r-2} + A_{r-2}(m^2-1)$. Тоді n можна записати у вигляді $n = a_k m^k + \dots + a_2 m^2 + a_1 m + a_0 = a_k((-1)^k + A_k(m+1)) + \dots + a_2((-1)^2 + A_2(m+1)) + a_1((-1)^1 + A_1(m+1)) + a_0 = (a_k A_k + \dots + a_2 A_2 + a_1 A_1)(m+1) + (-1)^k a_k + \dots + a_2 - a_1 + a_0$. Оскільки перший доданок ділиться на d, бо кратний $m+1$, то для подільності на d числа n необхідно й достатньо, щоб на d ділився і другий доданок $(-1)^k a_k + \dots + a_2 - a_1 + a_0$. □

30.

Нехай α_1, α_2, α_3, ... – нескінченна послідовність m-кових цифр, в якій є нескінченно багато цифр, відмінних від $m-1$ (тобто ми не розглядаємо послідовності, "хвіст" яких містить лише цифру $m-1$). Нескінченний ряд

$$\frac{\alpha_1}{m}+\frac{\alpha_2}{m^2}+\frac{\alpha_3}{m^3}+\cdots+\frac{\alpha_k}{m^k}+\cdots \tag{3.5}$$

називається *систематичним m-ковим дробом* (або просто m-ковим дробом) і звичайно позначається

$$0,\alpha_1\alpha_2\alpha_3\ldots\alpha_k\ldots\ . \tag{3.6}$$

Якщо в послідовності $\alpha_1\alpha_2\alpha_3\ldots$, починаючи з певного місця, зустрічаються лише нулі, то дріб (3.5) називається *скінченним*. У противному разі він називається *нескінченним*. Для скінченних дробів "хвіст" із нулів звичайно не виписують і замість (3.6) вживають скорочене позначення $0,\alpha_1\alpha_2\alpha_3\ldots\alpha_k$. Наприклад, дріб $0,011000\ldots$ (починаючи з 4-го місця йдуть лише нулі) може позначатись або $0,011$, або $0,0110$, або $0,01100$ і т.д.

Із нерівностей $0\le\alpha_i\le m-1$, $i=1,2,\ldots$ і того, що серед цифр дробу є відмінні від $m-1$, випливає, що

$$0\le\frac{\alpha_1}{m}+\frac{\alpha_2}{m^2}+\frac{\alpha_3}{m^3}+\cdots<\frac{m-1}{m}+\frac{m-1}{m^2}+\frac{m-1}{m^3}+\cdots=$$
$$\frac{m-1}{m}\left(1+\frac{1}{m}+\frac{1}{m^2}+\cdots\right)=\frac{m-1}{m}\cdot\frac{1}{1-\frac{1}{m}}=1.$$

Таким чином, ряд (3.5) завжди збігається і його сума α належить проміжку $[0,1)$. Говорять, що число α зображується дробом (3.6), або що дріб (3.6) дорівнює α, і пишуть $\alpha=0,\alpha_1\alpha_2\alpha_3\ldots\alpha_k\ldots$.

Теорема 3.2. *Кожне дійсне число $\alpha\in[0,1)$ зображується деяким m-ковим дробом. Таке зображення однозначне.*

Доведення. Існування зображення. Побудуємо ланцюжок рівностей

$$m\alpha = \alpha_1 + \beta_1, \text{ де } \alpha_1 = [m\alpha],\ \beta_1 = \{m\alpha\};$$

$$m\beta_1 = \alpha_2 + \beta_2, \text{ де } \alpha_2 = [m\beta_1],\ \beta_2 = \{m\beta_1\};$$

$$m\beta_2 = \alpha_3 + \beta_3, \text{ де } \alpha_3 = [m\beta_2],\ \beta_3 = \{m\beta_2\};\ \text{і т.д.}$$

За умовою теореми та означенням дробової частини числа всі числа $\alpha, \beta_1, \beta_2, \beta_3, \dots$ належать проміжку $[0, 1)$, тому всі числа $m\alpha, m\beta_1, m\beta_2, \dots$ належать проміжку $[0, m)$, а всі числа $\alpha_1 = [m\alpha], \alpha_2 = [m\beta_1], \alpha_3 = [m\beta_2], \dots$ – множині $\{0, 1, \dots, m-1\}$. Тому числа $\alpha_1, \alpha_2, \alpha_3, \dots$ можна розглядати як m-кові цифри.

Доведемо, що $\alpha = 0, \alpha_1\alpha_2\alpha_3\dots$, тобто що

$$\alpha = \frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \frac{\alpha_3}{m^3} + \cdots . \tag{3.7}$$

Для цього розглянемо різницю $\gamma_k = \alpha - (\frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \cdots + \frac{\alpha_k}{m^k})$. Оскільки $m^k\gamma_k = m^k\alpha - m^{k-1}\alpha_1 - m^{k-2}\alpha_2 - \cdots - \alpha_k = m^{k-1}(m\alpha - \alpha_1) - m^{k-2}\alpha_2 - \cdots - \alpha_k = m^{k-1}\beta_1 - m^{k-2}\alpha_2 - m^{k-3}\alpha_3 - \cdots - \alpha_k = m^{k-2}(m\beta_1 - \alpha_2) - m^{k-3}\alpha_3 - \cdots - \alpha_k = m^{k-2}\beta_2 - m^{k-3}\alpha_3 - \cdots - \alpha_k = \dots = m\beta_{k-1} - \alpha_k = \beta_k$ і $0 \le \beta_k < 1$, то $0 \le \gamma_k < \frac{1}{m^k}$. Тому $\gamma_k \to 0$ при $k \to \infty$. Отже, послідовність часткових сум ряду $\frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \cdots + \frac{\alpha_k}{m^k} + \cdots$ збігається до числа α, що й доводить рівність (3.7).

Єдиність зображення. Треба довести, що різні дроби зображують різні дійсні числа. Нехай послідовності цифр $\alpha_1, \alpha_2, \alpha_3, \dots$ і $\beta_1, \beta_2, \beta_3, \dots$ – різні, і нехай k – найменший номер позиції, в якій вони розрізняються (тобто $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}$, але $\alpha_k \ne \beta_k$). Без обмеження загальності можна вважати, що $\alpha_k > \beta_k$. Розглянемо різницю

$$\left(\frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \frac{\alpha_3}{m^3} + \cdots\right) - \left(\frac{\beta_1}{m} + \frac{\beta_2}{m^2} + \frac{\beta_3}{m^3} + \cdots\right) = \frac{\alpha_k - \beta_k}{m^k} + \left(\frac{\alpha_{k+1} - \beta_{k+1}}{m^{k+1}} + \frac{\alpha_{k+2} - \beta_{k+2}}{m^{k+2}} + \cdots\right) . \tag{3.8}$$

За означенням дробу серед цифр $\beta_{k+1}, \beta_{k+2}, \dots$ є нескінченно багато менших за $m-1$, а тому серед чисел $\alpha_{k+1} - \beta_{k+1}$, $\alpha_{k+2} - \beta_{k+2}$, … буде нескінченно багато більших за $-(m-1)$. Звідси випливає, що

$$\frac{\alpha_{k+1} - \beta_{k+1}}{m^{k+1}} + \frac{\alpha_{k+2} - \beta_{k+2}}{m^{k+2}} + \cdots > \frac{-(m-1)}{m^{k+1}} + \frac{-(m-1)}{m^{k+2}} + \cdots =$$

$$= -\frac{m-1}{m^{k+1}}\left(1+\frac{1}{m}+\frac{1}{m^2}+\cdots\right) = -\frac{m-1}{m^{k+1}}\cdot\frac{1}{1-\frac{1}{m}} = -\frac{1}{m^k}.$$

З іншого боку,

$$\frac{\alpha_k-\beta_k}{m^k} \geq \frac{1}{m^k}.$$

Із цих нерівностей для доданків правої частини рівності (3.8) отримуємо:

$$\left(\frac{\alpha_1}{m}+\frac{\alpha_2}{m^2}+\cdots\right)-\left(\frac{\beta_1}{m}+\frac{\beta_2}{m^2}+\cdots\right) > \frac{1}{m^k}-\frac{1}{m^k} = 0.$$

Таким чином, для чисел $\alpha = 0,\alpha_1\alpha_2\alpha_3\ldots$ і $\beta = 0,\beta_1\beta_2\beta_3\ldots$ виконується нерівність $\alpha-\beta>0$. Тому $\alpha\neq\beta$, що й треба було довести. □

31.

m-ковий дріб $\alpha = a,\alpha_1\alpha_2\alpha_3\ldots$ називається *періодичним*, якщо послідовність $\alpha_1\alpha_2\alpha_3\ldots$ його цифр є періодичною, тобто якщо існують такі числа $k\geq 0$ і $t\geq 1$, що для всіх $n>k$ виконується рівність $\alpha_n=\alpha_{n+t}$. Якщо для періодичного дробу $\alpha = a,\alpha_1\alpha_2\alpha_3\ldots$ серед таких k вибрати найменше k_0, то $\alpha_1\alpha_2\ldots\alpha_{k_0}$ називається *передперіодом* дробу α, а саме число k_0 – *довжиною передперіоду*. Аналогічно найменше з усіх можливих t число t_0 називається *довжиною періоду*, а набір цифр $\alpha_{k_0+1}\alpha_{k_0+2}\ldots\alpha_{k_0+t_0}$ – *періодом дробу* α.

Періодичний дріб, передперіод якого має нульову довжину, називається *чисто періодичним* дробом.

Періодичний дріб із довжиною передперіоду k і довжиною періоду t має вигляд

$$\alpha = a,\alpha_1\alpha_2\ldots\alpha_k\alpha_{k+1}\ldots\alpha_{k+t}\alpha_{k+1}\ldots\alpha_{k+t}\alpha_{k+1}\ldots.$$

Оскільки після передперіоду цифри регулярно повторюються, то для періодичних дробів використовують позначення $\alpha = a,\alpha_1\ldots\alpha_k(\alpha_{k+1}\ldots\ldots\alpha_{k+t})$.

Теорема 3.3. *В m-ковій системі числення кожне раціональне число зображується періодичним дробом. Навпаки, кожний періодичний дріб зображує певне раціональне число.*

Доведення. Нехай $\alpha = \frac{a}{b}$ – раціональне число. Нас цікавлять лише знаки після коми, тому можна вважати, що $0 \leq \frac{a}{b} < 1$. Із вправи 3.2 випливає, що перша цифра α_1 дробу $\frac{a}{b} = 0, \alpha_1\alpha_2\alpha_3\ldots$ дорівнює $\alpha_1 = [m\frac{a}{b}]$, тобто α_1 визначається з рівності $ma = \alpha_1 b + r_1$, $0 \leq r_1 < b$. Аналогічно, друга цифра α_2 визначається з рівності $mr_1 = \alpha_2 b + r_2$, $0 \leq r_2 < b$, третя – з рівності $mr_2 = \alpha_3 b + r_3$, $0 \leq r_3 < b$ і т.д. Але всі члени послідовності $a, r_1, r_2, r_3, \ldots$ належать скінченній множині $\{0, 1, 2, \ldots, b-1\}$, тому рано чи пізно якийсь із них повториться. Отже, існують такі натуральні числа k і t, що $r_k = r_{k+t}$. Але тоді $mr_{k+t} = mr_k = \alpha_{k+1}b + r_{k+1}$. З іншого боку, $mr_{k+t} = \alpha_{k+t+1}b + r_{k+t+1}$. Із однозначності ділення з остачею випливає, що $\alpha_{k+t+1} = \alpha_{k+1}$ і $r_{k+t+1} = r_{k+1}$. Аналогічно доводиться, що $\alpha_{k+t+2} = \alpha_{k+2}$ і $r_{k+t+2} = r_{k+2}$, і т.д. Отже, дріб $\alpha = 0, \alpha_1\alpha_2\alpha_3\ldots$ – періодичний.

Навпаки, нехай дріб $\alpha = 0, \alpha_1\ldots\alpha_k(\beta_1\ldots\beta_t)$ – періодичний. Позначивши для зручності $A = (\alpha_1\ldots\alpha_k)_m$, $B = (\beta_1\ldots\beta_t)_m$, ми можемо записати число α у вигляді ряду

$$\alpha = \frac{A}{m^k} + \frac{B}{m^k \cdot m^t} + \frac{B}{m^k \cdot m^{2t}} + \frac{B}{m^k \cdot m^{3t}} + \ldots.$$

Але тоді

$$\alpha = \frac{A}{m^k} + \frac{B}{m^{k+t}}\left(1 + \frac{1}{m^t} + \frac{1}{m^{2t}} + \ldots\right) = \frac{A}{m^k} + \frac{B}{m^{k+t}} \cdot \frac{1}{1 - \frac{1}{m^t}} = \frac{A(m^t - 1) + B}{m^k(m^t - 1)}.$$

Числа A і B – цілі, тому α – раціональне число. □

Наслідок 1. *У зображенні раціонального числа $\frac{a}{b}$ m-ковим дробом сума довжин періоду і передперіоду не перевищує b.*

З'ясуємо ще, коли раціональне число $\frac{a}{b}$ зображується в m-ковій системі числення скінченним дробом. Знову досить обмежитись випадком $0 \leq \frac{a}{b} < 1$. Крім того, вважаємо дріб $\frac{a}{b}$ нескоротним. Із рівності

$$\frac{a}{b} = 0, \alpha_1\alpha_2\ldots\alpha_k = \frac{\alpha_1}{m} + \frac{\alpha_2}{m^2} + \ldots + \frac{\alpha_k}{m^k} = \frac{\alpha_1 m^{k-1} + \alpha_2 m^{k-2} + \ldots + \alpha_k}{m^k}$$

одержуємо: $am^k = b(\alpha_1 m^{k-1} + \alpha_2 m^{k-2} + \ldots + \alpha_k)$. Отже, $b|am^k$. За твердженням 1.2(b) із взаємної простоти чисел a і b випливає, що $b|m^k$.

Навпаки, нехай для якогось k маємо $b|m^k$. Тоді m^k можна записати у вигляді $m^k = b \cdot b_1$, звідки

$$\frac{a}{b} = \frac{m^k a}{m^k b} = \frac{bb_1 a}{m^k b} = \frac{b_1 a}{m^k}.$$

За умовою $0 \leq \frac{a}{b} < 1$, тому $0 \leq b_1 a < m^k$ і запис числа $b_1 a$ в m-ковій системі містить не більше k цифр. Дописавши, в разі потреби, кілька нулів попереду, можемо вважати, що $b_1 a = (\alpha_{k-1}\alpha_{k-2}\ldots\alpha_1\alpha_0)_m = \alpha_{k-1}m^{k-1} + \alpha_{k-2}m^{k-2} + \ldots + \alpha_1 m + \alpha_0$. Але тоді

$$\frac{a}{b} = \frac{\alpha_{k-1}m^{k-1} + \alpha_{k-2}m^{k-2} + \ldots + \alpha_1 m + \alpha_0}{m^k} =$$

$$\frac{\alpha_{k-1}}{m} + \frac{\alpha_{k-2}}{m^2} + \ldots + \frac{\alpha_1}{m^{k-1}} + \frac{\alpha_0}{m^k} = (0, \alpha_{k-1}\alpha_{k-2}\ldots\alpha_1\alpha_0)_m,$$

тобто число $\frac{a}{b}$ зображується в m-ковій системі скінченним дробом.

Сформулюємо одержаний результат:

Теорема 3.4. *Нескоротний дріб $\frac{a}{b}$ зображується в m-ковій системі числення скінченним дробом тоді й лише тоді, коли $b|m^k$ для деякого натурального числа k.*