2 ДІЛЕННЯ ЦІЛИХ ЧИСЕЛ З ОСТАЧЕЮ

Теорема 1 (про ділення з остачею) Нехай $a, b \in \mathbb{Z}$, $b \neq 0$. Тоді існують єдині цілі числа q (*неповна частка*) і r (*остача*) такі, що $a = bq + r$ і $0 \le r < |b|$.

Доведення.

Спочатку доведемо існування чисел q і r. Якщо $a = 0$, то можна взяти $q = r = 0$. Тому далі будемо вважати $a \neq 0$.

Розглянемо першим випадок $a > 0$, $b > 0$ і доведемо індукцією по a. База індукції: $a < b$. В цьому випадку $a = b \cdot 0 + a$ і $0 \le a < b$. Перехід: нехай тепер $a \ge b$, звідки $a - b \ge 0$ і $a - b < a$, тому за припущенням індукції знайдуться такі q' і r', що $a - b = bq' + r'$ і $0 \le r' < b$, отже $a = b(q' + 1) + r'$. Нехай тепер $a \le 0$, але $-a \ge 0$ і за доведеним знайдуться такі q' і r', що $-a = bq' + r'$, $0 \le r' < b$. Звідси маємо $a = -bq' - r'$. Якщо $r' = 0$, то $a = -bq' + 0 = b(-q') + 0$ і все доведене. Якщо ж $1 \le r' < b$, то $a = b(-q') - b + b - r' = b(-q' - 1) + (b - r')$. Помітимо, що $-b < -r' \le -1$, тому $0 < b - r' \le b - 1$ і все доведене.

Нарешті, припустимо, що $b < 0$, тоді $-b > 0$ і можна знайти такі q' і r', що $a = (-b)q' + r'$ і $0 \le r' < -b$. Але тоді $a = (-b)q' + r'$ і $0 \le r' < |b|$, що й потрібно.

Залишилося довести єдиність. Припустимо зворотне: нехай $a = bq + r = bq' + r'$; тоді $b(q - q') = r - r'$. Якщо $q = q'$, то і $r = r'$. Якщо ж $q \neq q'$, то $|b| \cdot |q - q'| = |r - r'|$ і ліва частина $\ge |b|$. З іншого боку, $0 \le r, r' < |b|$, тому права частина не перевищує $|b|$, протиріччя.

Приклад 1 Обчислити частку q й остачу r від ділення числа -187 на число -13.

Розв'язання.

Оскільки $\frac{187}{13} = 14\frac{5}{13}$, то

$$-187 = 14\frac{5}{13} \cdot (-13) = \left(15 - \frac{8}{13}\right) \cdot (-13) = 15 \cdot (-13) + 8.$$

Отже, $q = 15$, $r = 8$.

Відповідь: $q = 15$, $r = 8$.

Приклад 2 Обчислити натуральне число b й остачу r від ділення числа $a = 19178$ на b, якщо частка від ділення a на b дорівнює 129.

Розв'язання.

Із рівності $19178 = 129 \cdot b + r$ маємо $b = \frac{19178 - r}{129} = 148 + \frac{86 - r}{129}$. Оскільки число b ціле, то $b \le 148$. З нерівності $0 \le r < b$ тепер отримуємо

$\frac{86}{129}=\frac{86-0}{129}\geq\frac{86-r}{129}>\frac{86-148}{129}=-\frac{62}{129}$. Але число $\frac{86-r}{129}$ має бути цілим. Тому $86-r=0$, звідки $r=86$ і $b=148$.

Відповідь: $r=86$, $b=148$.

Приклад 3 Обчислити натуральне число b і частку q від ділення числа $a=3616$ на b, якщо $q>1$ й остача від ділення a на b дорівнює 305.

Розв'язання.

З рівності $3616=qb+305$ маємо $qb=3311=7\cdot11\cdot43$. За умовою задачі $b>305$ і $b>3311$, бо $q>1$. Серед дільників числа 3311 є лише один, який задовольняє ці нерівності, а саме $11\cdot43=473$. Тому $b=473$ і $q=7$.

Відповідь: $b=473$, $q=7$.

Приклад 4 Непарне число m ділиться націло на 3. Чому дорівнює остача при діленні числа m на 6?

Розв'язання.

При діленні цілого числа на 6 можуть бути отримані остачі 0, 1, 2, 3, 4, 5. Тому будь-яке число можна подати в одному з таких виглядів:

$$6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5,\ \text{де } k\in\mathbb{Z}.$$

Із цих чисел кратні 3 тільки числа виду $6k$ і $6k+3$. Оскільки число m непарне, то воно може бути тільки виду $6k+3$.

Відповідь: 3.

Приклад 5 Доведіть, що серед п'яти послідовних цілих чисел є тільки одне, яке кратне 5.

Розв'язання.

Розглянемо п'ять послідовних цілих чисел: n, $n+1$, $n+2$, $n+3$, $n+4$. Оскільки модуль різниці будь-яких двох таких чисел менший від 5 і не дорівнює нулю, то він не ділиться націло на 5. Отже, усі п'ять чисел дають різні остачі при діленні на 5. Різних остач при діленні на 5 також 5. Отже, одне із цих чисел при діленні на 5 дає в остачі 0.

Зауваження. Міркуючи аналогічно, можна довести, що серед m послідовних цілих чисел є тільки одне, яке кратне m.

Приклад 6 Доведіть, що з $n+1$ натуральних чисел завжди можна вибрати два таких, що їхня різниця ділиться націло на n.

Розв'язання.

При діленні цілих чисел на n можна отримати n різних остач: 0, 1, …, $n-1$. Оскільки заданих чисел $n+1$, то щонайменше два з них дають однакові остачі при діленні на n. Тоді їхня різниця ділитиметься націло на n.

Цілі числа a і b називають *конгруентними за модулем* m ($m\in\mathbb{N}$), якщо остачі при діленні їх на число m рівні. Позначення: $a\equiv b\pmod m$ – *конгруенція*.

Приклад 7

$5\equiv8\pmod3$, $7\equiv-1\pmod4$, $18\equiv0\pmod9$, $25\equiv35\pmod5$.

Теорема 2 Для того, щоб цілі числа a і b були конгруентними за модулем m ($m\in\mathbb{N}$), необхідно і достатньо, щоб різниця $a-b$ ділилася націло на m.

Доведення.

Необхідність. За означенням, $a \equiv b \pmod m$, якщо $a = mq_1 + r$ і $b = mq_2 + r$. Тоді, $a - b = m(q_1 - q_2) \vdots m$.

Достатність. $a - b = m(q_1 - q_2) \vdots m$, отже $a = mq_1 + r$ і $b = mq_2 + r$.

Теорема 3 (властивості конгруенцій) Для будь-яких цілих a, b, c, d і натуральних m і n виконано:

1) якщо $a \equiv b \pmod m$, $b \equiv c \pmod m$, то $a \equiv c \pmod m$;
2) якщо $a \equiv b \pmod m$, то $a + c \equiv b + c \pmod m$;
3) якщо $a \equiv b \pmod m$, то $ac \equiv bc \pmod m$;
4) якщо $a \equiv b \pmod m$ і $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$;
5) якщо $a \equiv b \pmod m$ і $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$;
6) якщо $a \equiv b \pmod m$, то $a^n \equiv b^n \pmod m$.

Доведення.

1) $a \equiv b \pmod m$, отже $(a - b) \vdots m$ і $b \equiv c \pmod m$, отже $(b - c) \vdots m$. Тоді, $a - c = (a - b) + (b - c)$ і $(a - c) \vdots m$.
2) $a \equiv b \pmod m$, отже $(a - b) \vdots m$. Тоді, $a - b = (a - c) - (b - c)$.
3) $a \equiv b \pmod m$, отже $(a - b) \vdots m$. Тоді, $ac - bc = c(a - b) \vdots m$.
4) $a \equiv b \pmod m$, отже $(a - b) \vdots m$ і $c \equiv d \pmod m$, отже $(c - d) \vdots m$. Тоді, $(a - b) \pm (c - d) = (a \pm c) - (b \pm d)$.
5) $a \equiv b \pmod m$, отже $a = mq_1 + b$ і $c \equiv d \pmod m$, отже $c = mq_2 + d$. Тоді, $ac - bd = (mq_1 + b)(mq_2 + d) - bd = m(mq_1q_2 + bq_2 + dq_1) \vdots m$.
6) $a \equiv b \pmod m$, отже $(a - b) \vdots m$. Тоді,
$$a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1}\right) \vdots m.$$

Приклад 8 Чому може дорівнювати остача при діленні числа n^4 на 5, $n \in \mathbb{Z}$?

Розв'язання.

Має місце одна з п'яти конгруенцій:

$$n \equiv 0 \pmod 5,$$
$$n \equiv 1 \pmod 5,$$
$$n \equiv 2 \pmod 5,$$
$$n \equiv 3 \pmod 5,$$
$$n \equiv 4 \pmod 5.$$

Скориставшись властивістю 6 конгруенцій, отримаємо:

$$n^4 \equiv 0 \pmod 5,$$
$$n^4 \equiv 1 \pmod 5,$$

$$n^4 \equiv 16 \pmod 5 \equiv 1 \pmod 5,$$
$$n^4 \equiv 81 \pmod 5 \equiv 1 \pmod 5,$$
$$n^4 \equiv 256 \pmod 5 \equiv 1 \pmod 5.$$

Відповідь: 0 або 1.

Приклад 9 Остача від ділення трицифрового числа $n = \overline{2bb}$ на деяке одноцифрове число дорівнює 8, знайдіть число n.

Розв'язання.

Оскільки остача від ділення дорівнює 8, тоді розглянемо конгруенцію за модулем 9: $n \equiv 8 \pmod 9$, тоді $200 + 10b + b \equiv 8 \pmod 9$, $200 + 11b \equiv 8 \pmod 9$, $11b \equiv -192 \pmod 9 \equiv 6 \pmod 9 \equiv 33 \pmod 9$, звідки $b \equiv 3 \pmod 9$.

Отже, шукане $n = 233$.

Відповідь: 233.

Приклад 10 Доведіть, що при будь-якому натуральному n значення виразу $2^{4n+3} + 13 \cdot 3^{2n}$ кратне 7.

Розв'язання.

Перетворимо вихідний вираз наступним чином:

$$2^{4n+3} + 13 \cdot 3^{2n} = 8 \cdot 16^n + 13 \cdot 9^n.$$

Очевидно, що $16 \equiv 9 \pmod 7$. Застосовуючи до цієї конгруенції низку властивостей, отримаємо:

$$16^n \equiv 9^n \pmod 7,$$
$$8 \cdot 16^n \equiv 8 \cdot 9^n \pmod 7,$$
$$8 \cdot 16^n + 13 \cdot 9^n \equiv 8 \cdot 9^n + 13 \cdot 9^n \pmod 7,$$
$$8 \cdot 16^n + 13 \cdot 9^n \equiv 21 \cdot 9^n \pmod 7 \equiv 0 \pmod 7.$$

Приклад 11 Знайдіть остачу від ділення числа 7^{29} на 5.

Розв'язання.

Запишемо очевидну конгруенцію і застосуємо до неї низку властивостей:

$$7^2 \equiv -1 \pmod 5,$$
$$\left(7^2\right)^{14} \equiv (-1)^{14} \pmod 5,$$
$$7^{28} \equiv 1 \pmod 5,$$
$$7^{29} \equiv 7 \pmod 5 \equiv 2 \pmod 5.$$

Відповідь: 2.

Приклад 12 Знайдіть остачу від ділення 2012^{2013} на 3.

Розв'язання.

Розглянемо очевидну конгруенцію $2012 \equiv -1 (\mathrm{mod}\ 3)$, тоді $2012^{2013} \equiv (-1)^{2013} (\mathrm{mod}\ 3) \equiv -1 (\mathrm{mod}\ 3) \equiv 2 (\mathrm{mod}\ 3)$. Отже, остача від ділення дорівнює 2.

Відповідь: 2.