4. Арифметика остатков

4.1 Число x даёт при делении на 7 остаток 5. Какой остаток дают при делении на 7 число $x+4$? число $2x$? число $4x+9$? число x^2-x? число x^3? число x^{100}?

▷ По условию $x = 7k+5$ для некоторого k. Тогда (1) $x+4 = 7k+9 = 7(k+1)+2$ и даёт остаток 2 при делении на 7. Далее, (2) $2x = 7\cdot 2k+10 = 7(2k+1)+3$ и потому $2x$ даёт остаток 3 при делении на 5. (3)$4x+9 = 4(7k+5)+7+2 = 4\cdot 7k+4\cdot 5+7+2 = 7\cdot 4k+29 = 7\cdot(4k+4)+1$, так что остаток равен 1. (4) $x^2-x = (7k+5)^2-(7k+5) = 7k(7k+5)+5(7k+5)-7k-5 = 7k(7k+5)+5\cdot 7k+5\cdot 5-7k-5 = 7(k(7k+5)+5k-k)+20 = 7(\ldots)+14+6 = 7(\ldots+2)+6$, так что остаток снова равен 6. (5) $x^3 = (7k+5)^3 = (7k+5)(7k+5)(7k+5)$. В этом выражении, если раскрыть скобки, все члены будут кратны 7, и их можно даже не выписывать, кроме одного $5\cdot 5\cdot 5 = 125 = 17\cdot 7+6$, так что остаток равен 6. Для x^{100}: будем последовательно выписывать разные степени: $x, x^2, x^3, x^4, x^5, x^6, x^7, \ldots$ дают остатки 5, 4, 6, 2, 3, 1, 5 ... и дальше всё повторяется с периодом 6, так что x^{100} будет давать тот же остаток, что и x^4 (разница 96 в степенях делится на 6), то есть 2. ◁

По существу, мы систематически выбрасываем кратные 7, потому что они не влияют на ответ. Вообще вместо какого-то x, дающего остаток 5 при делении на 7, можно взять число 5, и получить ответ почти сразу. Мы сейчас объясним, почему это законно.

Определение. Говорят, что два числа x и y *сравнимы по модулю* n, если их разница делится на n.

Здесь n — целое положительное число (мы на него делим). Не имеет значения, из какого числа вычитать какое: если $b-a$ делится на n, то и $(a-b) = -(b-a)$ тоже делится на n (только частное меняет знак).

Запись: $x \equiv y \pmod{n}$; знак $\equiv$ читают как «сравнимы» или «эквивалентны», это синонимы (значат одно и то же).

Математики говорят, что отношение сравнимости (по данному модулю) является *отношением эквивалентности*. На их языке это означает выполнение трёх свойств:

- *рефлексивность*: каждое число эквивалентно самому себе;
- *симметричность*: если x эквивалентно y, то y эквивалентно x;
- *транзитивность*: если x и y эквивалентны z, то x эквивалентно y.

Эти три свойства гарантируют возможность разбиения всех объектов на непересекающиеся *классы эквивалентности*, при этом элементы одного класса будут эквивалентны друг другу, а разных — нет. В самом деле, для каждого x рассмотрим все элементы, эквивалентные x, они все эквивалентны друг другу (транзитивность), и среди них есть x. Элементы двух классов не эквивалентны друг другу (иначе классы совпадают по симметричности и транзитивности).

4.2 Закончите фразу: «два числа x и y сравнимы по модулю n, если их остатки...». Проверьте свойства отношения эквивалентности (рефлексивность, симметричность, транзитивность). Сколько будет классов эквивалентности?

▷ «...при делении на n равны». Отсюда очевидны все свойства отношения эквивалентности. Классов будет столько, сколько различных остатков, то есть n. ◁

Возможность систематического выбрасывания кратных n при действиях по модулю n гарантируется такой задачей:

4.3 Докажите, что если $a \equiv b \pmod n$, то $a + c \equiv b + c \pmod n$ и $ac \equiv bc \pmod n$. Докажите, что если $a \equiv b \pmod n$ и $b \equiv c \pmod n$, то $a \equiv c \pmod n$.

▷ (1) Если $b - a$ делится на n, то $(b + c) - (a + c)$ делится на n, потому что это то же самое число. (2) Здесь $bc - ac = (b - a)c$ делится на n, потому что один сомножитель делится на n. (3) Если $b - a$ делится на n, а также $c - b$ делится на n, то и сумма $(b - a) + (c - b) = c - a$ делится на n. ◁

4.4 Докажите, что если $a \equiv b \pmod n$ и $c \equiv d \pmod n$, то $a+c \equiv b+d \pmod n$ и $ac \equiv bd \pmod n$.

▷ Можно заметить, что если $b = a + kn$ и $d = c + ln$, то $b + d = a + c + (k + l)n$, поэтому $b + d \equiv a + c \pmod n$. Для произведения $bd = (a + kn)(c + ln) = ac + n(k + l + kln)$, поэтому $bd \equiv ac \pmod n$.

Но можно и проще: предыдущая задача позволяет заменять в сумме одно слагаемое на сравнимое по модулю n, и сумма не меняется по модулю n, после чего можно заменить и другое, она снова не изменится. Аналогично и для произведения. ◁

Эта задача показывает, что если в любом арифметическом выражении, содержащем сложение и умножение, заменить какие-то члены на

эквивалентные по модулю n (один или много раз), то значение выражения тоже заменится на эквивалентное. Математики сказали бы, что арифметические операции «корректно определены на классах эквивалентности».

▷ Можно сказать, что выбрав модуль n для сравнений, мы надеваем специальные очки, через которые мы не отличаем числа, различающиеся на кратные n, и потому позволяем себе всюду выбрасывать числа, кратные n (прибавлять и вычитать любое кратное n). Правильное вычисление остаётся правильным и в этих очках — но и неправильное, в котором ошибки кратны n, тоже покажется правильным — хотя правильным в нём будет только остаток по модулю n. ◁

4.5 Можно ли, продолжая предыдущую задачу, утверждать, что в её предположениях $a - c \equiv b - d \pmod{n}$ и $a/c = b/d \pmod{n}$?

▷ Первое верно (например, можно заметить, что $-c \equiv -d \pmod{n}$, умножая сравнение на -1, а потом сложить). Второе же не имеет смысла (по крайней мере пока): числа a/c и b/d вообще могут быть не целыми, так что для них сравнение по модулю не определено. (И если даже случайно и получатся целые, то тоже может быть неверно: $5 \equiv 10 \pmod{5}$, но $5/5 \not\equiv 10/5 \pmod{5}$.) Как и когда имеет смысл делить сравнения, мы ещё обсудим. ◁

4.6 Найдите остаток от деления на 7 чисел 8^{100} и 6^{100}.

▷ Поскольку $8 \equiv 1 \pmod{7}$ и $6 \equiv -1 \pmod{7}$, можно с тем же успехом искать остаток от деления 1^{100} и $(-1)^{100}$, оба числа равны 1, так что оба искомых остатка равны 1. ◁

4.7 Найдите остаток от деления числа 2^{100} на 7.

▷ Поскольку $2^3 \equiv 1 \pmod{7}$, то множители 2^3 по модулю 7 можно сокращать, а $100 = 3 \cdot 33 + 1$, поэтому останется единственный множитель 2, который и будет искомым остатком. ◁

4.8 Будем брать степени какого-то фиксированного числа a по модулю b (другими словами, брать остатки $a^k \bmod b$). С какого-то момента они начинают повторяться по циклу (одна и та же группа повторяется снова и снова). Почему так обязательно случится?

• Скажем, для степеней двойки по модулю 10 (последние цифры): 1, 2, 4, 8, [1]6, [3]2, [6]4, [12]8,...: группа 2, 4, 8, 6 повторяется (а начальная единица — нет).

▷ Каждое следующее число получается из предыдущего умножением на a. Рано или поздно остатки по модулю b повторятся, и потом уже

всё пойдёт по тому же пути (потому что мы можем умножать остаток на a по модулю b). ◁

4.9 Докажите, что число $2^{1001} + 3^{1001}$ делится на 5.

▷ Можно просто вычислить соответствующие остатки, как в предыдущей задаче. Но можно и сразу заметить, что $3 \equiv (-2) \pmod 5$, поэтому выражение сравнимо с $2^{1001} + (-2)^{1001} = 0$. (Внимание: тут важно, что показатель степени 1001 нечётный.) ◁

• То же самое верно (и по тем же причинам) для любых целых положительных a и b: число $a^n + b^n$ при нечётном n делится на $a + b$. Это же можно усмотреть и из формулы

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \ldots - ab^{n-2} + b^{n-1}),$$

которая верна при нечётном n и проверяется перемножением скобок в правой части, там всё посокращается. (Что будет при чётном n?)

4.10 Докажите, что если $a \equiv b \pmod n$, то $a \equiv b \pmod{n'}$ для любого n', делящего n.

▷ Если число $a - b$ делится на n, то оно делится и на любой делитель n' числа n. ◁

4.11 Докажите, что если $a \equiv b \pmod c$, то $ka \equiv kb \pmod{kc}$ (здесь мы предполагаем, что k и c — положительные целые числа). Верно ли обратное?

▷ Если $a - b$ делится на c, то число $(a - b)/c$ целое. Но это же число можно записать и как $k(a-b)/kc$, так что $k(a-b)$ делится на k. То же самое в обратном направлении: если $ka - kb$ делится на kc, то $(ka - kb)/kc = (a - b)/c$ будет целым. Так что и обратное верно. ◁

4.12 Можно ли сокращать сравнения на ненулевой множитель? Верно ли, что если $ka \equiv kb \pmod c$, а $k \not\equiv 0 \pmod c$, то $a \equiv b \pmod c$?

▷ Не всегда. Например, $2 \cdot 3 \equiv 2 \cdot 8 \pmod{10}$, и $2 \not\equiv 0 \pmod{10}$, но $3 \not\equiv 8 \pmod{10}$. ◁

• Мы потом увидим, что иногда сокращать можно: если сокращаемый множитель взаимно прост с модулем сравнения.

4.13 Покажите, что записанное обычным образом (в десятичной системе) целое положительное число сравнимо по модулю 9 с суммой своих цифр. Как из этого вывести признаки делимости на 9 и на 3? (Они

говорят, что число делится на 9 [на 3] тогда и только тогда, когда сумма его цифр делится на 9 [на 3].)

▷ Числа $10, 100, 1000, \ldots$ все сравнимы с 1 по модулю 9 (потому что $100\ldots0 - 1 = 99\ldots9$ делится на 9. Можно ещё заметить, что $10 \equiv 1 \pmod 9$ и потому $10^k \equiv 1^k \equiv 1 \pmod 9$.

Поэтому, скажем,

$$2357 = 2{\cdot}1000+3{\cdot}100+5{\cdot}10+7{\cdot}1 \equiv 2{\cdot}1+3{\cdot}1+5{\cdot}1+7{\cdot}1 \equiv 2+3+5+7 \pmod 9,$$

и вообще любое число сравнимо со своей суммой цифр по модулю 9, так что если одно делится на 9, то и другое тоже. Сравнимость по модулю 9 влечёт за собой сравнимость по модулю 3, так что для 3 годится то же рассуждение. ◁

4.14* Можете ли вы предложить какие-то признаки делимости на 4, 8, 11, которые бы реально упрощали выяснение делимости? (Имеется в виду — без калькулятора и даже по возможности без бумаги и карандаша.)

▷ Для проверки делимости на 4 можно оставить только две последние цифры (потому что 100 делится на 4), для проверки делимости на 8 — три последние (и их уже делить честно). Поскольку $10 \equiv -1 \pmod{11}$, то для проверки делимости на 11 можно вычислить сумму цифр с чередующимися знаками (из суммы цифр на чётных местах вычесть сумму на нечётных). ◁

Иногда на обложках тетрадей печатают таблицу умножения натуральных чисел. (Таблицу сложения не печатают — видимо, считают, что это слишком просто.) Ясно, что в неё нельзя включить все возможные пары сомножителей, их бесконечно много. Однако для остатков по модулю n (если мы не различаем сравнимые по модулю n числа) такие таблицы составить можно, это будет таблица $n \times n$ (не считая заголовка). Мы уже по существу составляли такую таблицу для $n = 2$ с «чётом» и «нечетом»; теперь мы могли бы сказать, что это остатки 0 и 1 и каждый из остатков символизирует все сравнимые с ним числа.

4.15 Составьте такие таблицы (сложения и умножения) для $n = 3, 4, 5, 6, 7, 10$. (Их даже имеет смысл сохранить для следующих задач.)

▷ Вот эти таблицы (сначала для модулей 3, 4, 5, потом для 6, 7 и потом для 10). Последнюю таблицу можно иногда увидеть как таблицу умножения на школьных тетрадках, если смотреть только на последнюю цифру произведения.

	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

◁

4.16 Глядя в таблицу умножения по модулю 3, найдите в ней доказательство такого утверждения: если произведение двух целых чисел делится на 3, то одно из них делится на 3. Верно ли аналогичное утверждение для 4, 5, 6, 7, 10?

▷ Интересующее нас утверждение можно переформулировать так: если оба сомножителя не делятся на 3, то и произведение не делится на 3. Другими словами, нас интересует произведение *ненулевых* остатков,

так что на первую строку и первый столбец (не считая тех, что с множителями, то есть в квадратной части таблицы) не смотрим. А в остальных четырёх клеточках только 1 и 2, нулей нет.

Для $n = 4$ есть нуль $2 \cdot 2$, для $n = 6$ нули тоже есть (скажем, $2 \cdot 3$), для $n = 10$ тоже (скажем, $2 \cdot 5$). А для $n = 5$ и $n = 7$, как можно убедиться, посмотрев на таблицы, нулей нет. ◁

4.17 Какова может быть последняя цифра положительного целого числа n в десятичной записи, чтобы число n^2 кончалось на ту же цифру?

▷ Смотрим на диагональ (произведение чисел на себя) в последней таблице, и находим ответы (клетки, где стоит то же число, что и в заголовке таблицы): 0, 1, 5, 6. ◁

4.18* Найдите трёхзначное число, квадрат которого оканчивается на это число (то есть $n^2 \equiv n \pmod{1000}$). (Числа 000 и 001 за трёхзначные не считаются.)

▷ Удобно искать нужное число с конца. Мы уже знаем, что оно должно заканчиваться на 0, 1, 5, 6. Попробуем, скажем, 5 (тогда уж точно 001 и 000 не получатся). Какая может быть предпоследняя цифра?

$$(10k + 5)^2 = 100k^2 + 100k + 25$$

так что квадрат числа, оканчивающегося на 5, всегда оканчивается на 25, и со второй цифрой выбора нет. С третьей:

$$(100k + 25)^2 = 10000k^2 + 5000k + 625,$$

так что квадрат числа, оканчивающегося на 25, оканчивается на 625. Получаем ответ: $625^2 = 390\,625$.

Точнее сказать, это один из ответов. В задаче про это не спрашивалось, но можно пытаться найти все: $x^2 \equiv x \pmod{1000}$ означает, что $x^2 - x = x(x-1)$ делится на 8 и на 125. Если $x(x-1)$ делится на 8, то один из сомножителей (который чётен) делится на 8, получаем, что $x \equiv 0$ или $x \equiv 1$ по модулю 8. То же самое по модулю 125. Получаем 4 комбинации остатков по модулю 8 и 125 (см. дальше «китайскую теорему об остатках»), и четыре ответа: 000, 001, 625, 376 ($376^2 = 141\,376$) ◁

4.19 Какие последние цифры бывают у целых положительных чисел, которые делятся на 6? Какие остатки может давать число, делящееся на 2, при делении на 6? (Ответы на оба вопроса можно увидеть прямо по таблицам умножения, если правильно в них посмотреть.)

▷ Надо посмотреть в таблице умножения по модулю 10 тот ряд (столбец или строку), где умножают на 6, там стоят числа 0, 2, 4, 6, 8.

Для таблицы умножения по модулю 6 надо посмотреть ряд, где множат на 2, там стоят числа 0, 2, 4. ◁

4.20* Докажите, что квадрат одного целого числа не может быть втрое больше квадрата другого целого числа (за исключением случая, когда оба числа равны нулю).

▷ Это соответствует иррациональности числа $\sqrt{3}$. ◁

▷ Пусть $x = a^2 = 3b^2$, и $x \neq 0$. Возьмём минимальное такое x. Раз a^2 делится на 3, то и a делится на 3 (потому что ненулевые остатки в квадрате дают ненулевые), $a = 3z$. Тогда $a^2 = 9z^2 = 3b^2$, и $x/3 = 3z^2 = b^2$, так что x не минимальное — противоречие. ◁

4.21 Уравнение $x^2 + y^2 = 1003$ не имеет решений в целых числах (другими словами, число 1003 нельзя представить в виде суммы двух квадратов). Как в этом убедиться, не перебирая все варианты?

▷ Можно посмотреть на него по модулю 4: любой квадрат даёт остаток 0 или 1 при делении на четыре (в зависимостости от чётности), поэтому сумма двух квадратов может давать остаток 0, 1, или 2, но не 3 (как у 1003) ◁

▷ А что для других чисел (не только 1003)? Математики знают ответ (в терминах разложения на простые множители, о котором дальше): все простые числа вида $4k + 3$, входящие в разложение n, должны входить в чётной степени (парами), тогда можно представить n в виде суммы двух квадратов (а иначе — нельзя). Но это не так просто доказать. ◁