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 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?

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 $a \equiv c \pmod n$.

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 $ac \equiv bd \pmod n$.

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 $a/c = b/d \pmod n$?

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

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

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).

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

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

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 $a \equiv b \pmod{c}$?

• 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].)

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.)

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.)

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?

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

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.)

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.)

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 $\sqrt{3}$. ◁

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?

▷ 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. ◁