Константин Кохась

МИНУС НА МИНУС

– Для кредитов, которые собирается выдавать наш заказчик коллега Спрудль, получается уравнение $x^2 = 5476$, – сообщил дятел Спятел, глядя в бумажку.

– Не умею я так быстро считать! – пожаловался таракан Кузька Бусеньке. – Многозначные числа вгоняют меня в сон.

– И не надо! – сказала Бусенька. – Каждый должен хорошо делать свою работу. Громоздкие вычисления – не твоя специализация. Зато с небольшими числами ты оперируешь очень шустро. Значит, тебе нужно заниматься *модулярной арифметикой*!

– Чем-чем?

– Вычислениями с остатками! Ты же умеешь складывать и умножать остатки?

– Конечно, умею.

– Вот и выбери небольшое число, причём лучше простое, например 7 или 13, и специализируйся на вычислениях с остатками по модулю 7 или 13.

– Что за шум, не отвлекайтесь! – неодобрительно сказал дятел Спятел. – Мы говорили о том, что эффективность кредитов коллеги Спрудля зависит от уравнения $x^2 = 5476$. Как и положено квадратному уравнению, оно имеет два корня: $x = 74$ и $x = -74$. Первый корень означает отвратительное обогащение нашего заказчика. А второй корень ведёт к его умеренному обнищанию. Какой же корень следует взять? Этот выбор мы предоставим… самому́ заказчику! Причём по умолчанию мы подсунем ему отрицательный корень! А поскольку в порыве энтузиазма коллега Спрудль жмёт на кнопки, не думая…

– Тебе не кажется, что это… не совсем честно? – усомнилась Огрыза.

– Это здорово! – тихонечко сказал Кузька Бусеньке. – Я обнаружил, что по модулю 7 уравнение $x^2 = 2$ тоже имеет два корня: $3^2 \equiv 2 \pmod 7$ и $4^2 \equiv 2 \pmod 7$. Получается, что один из этих корней положительный, а другой отрицательный?

– Зачем тебе отрицательные остатки? – прошептала Бусенька. – Если хочешь, ты их все можешь считать отрицательными – вместо 1, 2, 3, 4, 5, 6 запиши -6, -5, -4, -3, -2, -1, и готово!

– А складывать как?

– Как обычно: $(-5)+(-3)=-8\equiv -8+7\equiv -1 \pmod 7$. И умножать так же: $(-5)\cdot(-3)=15\equiv 15-7\cdot 3\equiv -6 \pmod 7$.

– Я думаю, нас не должно огорчать то, что счёт коллеги Спрудля начнёт стремительно уменьшаться, – уверенно сказал дятел Спятел. – Он своими собственными щупальцами распорядится переводить деньги в благотворительный фонд!

– Жульничество какое-то, – сказал Кузька. – Зачем это нужно?

– Ну мало ли... Хочешь, например, подсчитать, чему равно 6^{10}, и сразу получаешь ответ: $6^{10}\equiv(-1)^{10}\equiv \equiv 1 \pmod 7$.

– Я не вижу никаких плюсов от деятельности коллеги Спрудля! – продолжал нагнетать дятел Спятел. – Только минусы!

– Это какие-то фальшивые минусы, – сказал Кузька Бусеньке, – не может так быть, чтобы всё было отрицательным.

– Тогда назначь половину остатков отрицательными, а другую половину положительными: 1, 2, 3, –3, –2, –1.

– Выглядит поинтереснее, – согласился Кузька. – Хотя... что же это получается? Произведение положительных остатков 2 и 3 равно –1?!

– Какие-то у тебя сомнительные методы, – проворчала Огрыза.

– Это неправильные минусы, – сказал Кузька, – нам, насекомым, такие минусы не нужны! Мы ценим только настоящие минусы! – И Кузька уполз под диван поразмышлять о природе Настоящих Минусов.

* * *

Бурные дискуссии, посвящённые проблеме изведения счетов коллеги Спрудля, уже давно закончились, когда, наконец, Кузька вылез из-под дивана.

– Я провёл кучу вычислений и всё понял! – сообщил Кузька. – Решение, можно сказать, было на поверхности! Например, по модулю 7 уравнение $x^2=a$ имеет корни только при $a=1, 2, 4$ и не имеет корней при $a=3, 5, 6$. Знаете, что это значит? Что если рассматривать ненулевые остатки по модулю простого числа p, то ровно для половины всех остатков a уравнение $x^2=a$ имеет решения и для половины не имеет!

– Как это грустно, когда у задачи нет решения, – вздохнул дятел Спятел.

– А почему ровно в половине случаев оно всё же есть? – поинтересовалась Огрыза.

– Не знаю, – ответил Кузька, – я установил этот факт экспериментально.

– А я могу доказать, – сказала Бусенька. – Рассмотрим ненулевые остатки по простому модулю p. Поскольку $x^2 = (-x)^2$, количество остатков, которые можно записать в виде x^2, не больше половины от числа всех остатков, то есть не больше $\frac{p-1}{2}$. С другой стороны, все остатки

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

различны, потому что равенство $a^2 \equiv b^2 \pmod{p}$ возможно, только если $(a-b)(a+b) \equiv 0 \pmod{p}$, то есть при $a = b$ или при $a = -b$ (ведь p простое). Таким образом, количество остатков, которые можно записать в виде x^2, в точности равно $\frac{p-1}{2}$. А тогда тех, которые нельзя записать в таком виде, тоже $\frac{p-1}{2}$.

– Ну… эээ… ясно, – сказал Кузька и зевнул, – только не путай меня своими отрицательными остатками! У тебя неправильные минусы! А *правильно* определять отрицательный остаток вот как: отрицательными следует считать только те ненулевые остатки a, для которых уравнение $x^2 = a$ не имеет решения. Например, по модулю 7 остатки 1, 2, 4 – положительные, а остатки 3, 5, 6 – отрицательные.

– Разве бывают неправильные определения? – спросил дятел Спятел.

– Бывают! – подтвердила Бусенька. – Когда придаём новый смысл уже существующему слову, этот смысл не должен слишком контрастировать с его другими смыслами.

– Чем же *это* определение правильное? – спросила Огрыза.

– Оно правильное, потому что для него выполняется… Правило Знаков! – воскликнул Кузька. – Произведение двух положительных или двух отрицательных остатков всегда положительно, а произведение положительного и отрицательного остатка – отрицательно. Я это проверил полным перебором.

– Потрясающе, – похвалила Огрыза. – А почему?

– То, что плюс на плюс будет плюс, – это понятно, – вмешался дятел Спятел. – Если $a=x^2$ и $b=y^2$ – положительные остатки, то и $ab=(xy)^2$ – тоже положительный остаток.

– Остальные случаи лишь чуточку хитрее, – сказала Бусенька. – Пусть x_1, x_2, ... – все положительные остатки, а y_1, y_2, ... – все отрицательные, и a – один из положительных остатков. Тогда все остатки ax_1, ax_2, ... , ay_1, ay_2, ... различны и не равны 0, поскольку по простому модулю p при ненулевых a равенство $au\equiv av \pmod p$ означает, что $u=v$. Но мы уже знаем, что ax_1, ax_2, ... положительны, и их ровно столько, сколько должно быть положительных остатков. Тогда все остальные остатки, то есть ay_1, ay_2, ..., отрицательны! Это и значит, что плюс на минус будет минус!

$\underbrace{ax_1, ax_2, \ldots}_{\text{положительные, и их ровно половина}}$ $\underbrace{ay_1, ay_2, \ldots}_{\text{значит, это в точности все отрицательные}}$

Если же b – отрицательный остаток, то bx_1, bx_2,..., by_1, by_2,..., тоже все различны, причём, как мы доказали, bx_1, bx_2,... отрицательны. Так как этих остатков ровно половина, остальные остатки by_1, by_2,... положительны! То есть минус на минус будет плюс!

$\underbrace{bx_1, bx_2, \ldots}_{\text{отрицательные, и их ровно половина}}$ $\underbrace{by_1, by_2, \ldots}_{\text{значит, это в точности все положительные}}$

– А остаток -1 положительный или отрицательный? – спросил дятел Спятел.

– Как повезёт, – ответил Кузька. – По модулю 7 уравнение $x^2=-1$ не имеет решений, значит, отрицательный. А по модулю 13 положительный: $5^2=25\equiv$ $\equiv -1 \pmod{13}$.

– Жаль, – сказала Огрыза.

– Очень жаль, – согласился Кузька. – Ведь если бы для всех простых p остаток -1 был отрицательным, то при решении квадратного уравнения $x^2=a$ с положительным a один корень всегда оказывался бы положительным, а другой – отрицательным! Например, для $p=7$ это так, и уравнение $x^2=2 \pmod 7$ имеет положительный корень 4 и отрицательный корень 3!

– Красотища! – сказала Бусенька. – Простые числа вида $4k+3$ мне всегда нравились немножко больше остальных.

Художник Инга Коржнева