$+ 38qr + r^2$ дает при делении на 19 такой же остаток, как и r^2.)

В нижней строке таблицы один раз присутствует число 0 и по два раза – числа 1, 4, 5, 6, 7, 9, 11, 16 и 17. Ненулевые остатки от деления квадратов целых чисел на простое число $p > 2$ называют *квадратичными вычетами* по модулю p. Все другие ненулевые остатки – *квадратичные невычеты* (при $p = 19$ это 2, 3, 8, 10, 12, 13, 14, 15 и 18).

Поскольку сумма никаких двух из чисел 1, 4, 5, 6, 7, 9, 11, 16 и 17 не кратна 19, приходим к выводу: сумма квадратов двух целых чисел кратна 19 в том и только том случае, когда слагаемые кратны 19.

Упражнение 6. Если p – простое число, $p > 2$, то существует $(p-1)/2$ квадратичных вычетов и ровно столько же квадратичных невычетов по модулю p. Докажите это.

Свойство простых чисел, не являющихся суммами двух квадратов

Как относиться к трудностям? В области неведомого надо рассматривать трудности как скрытый клад! Обычно: чем труднее, тем полезнее. Не так ценно, если трудности возникают от твоей борьбы с самим собой. Но когда трудности исходят от увеличившегося сопротивления предмета – это прекрасно!!

А.И.Солженицын

Чем больше по величине простое число p, тем больше квадратичных вычетов по модулю p. Поэтому пора менять метод исследования: если мы не желаем погрязнуть в нескончаемых вычислениях, то должны каким-то одним общим рассуждением охватить числа 3, 7, 11, 19 и многие другие простые числа.

Пока не вполне ясно, что это за числа и чем они отличаются от чисел 2, 5, 13, 17,... Впрочем, одно отличие очевидно: числа 3, 7, 11, 19 не представимы, а числа 2, 5, 13, 17 представимы в виде суммы квадратов двух целых чисел. Кроме того, простые числа $p = 3, 7, 11, 19$ обладают, как мы уже доказали, тем свойством, что если сумма квадратов целых чисел кратна p, то каждое из слагаемых кратно p. Продолжив (довольно утомительные, если не использовать компьютер) вычисления, можно доказать это свойство для $p = 23, 31, 43, 47, 59, 67, 71, 79, 83, 87$. Осечки ни разу не будет:

Теорема 2. *Если простое число p не представимо в виде суммы двух квадратов и если сумма квадратов $x^2 + y^2$ кратна p, то каждое из целых чисел x, y кратно p.*

Мы получим эту теорему как одно из следствий теории целых гауссовых чисел. Поскольку это не так уж просто, давайте отвлечемся на некоторое время от теоремы 2 и обратим внимание на другое свойство рассматриваемых простых чисел 3, 7, 11,..., 83, 87: *при делении на 4 они дают остаток 3.*

Числа вида $4n + 3$

В виде суммы двух квадратов не представимы не только простые числа, которые при делении на 4 дают остаток 3, но и вообще все числа 3, 7, 11, 15, 19, 23, 27,...:

Теорема 3. *Всякое представимое в виде суммы квадратов двух целых чисел нечетное число при делении на 4 дает остаток 1, а не 3.*

Доказательство. Из двух квадратов, сумма которых нечетна, обязательно один четен, а другой нечетен. Квадрат четного числа нацело делится на 4, а квадрат нечетного числа при делении на 4 дает остаток 1 (проверьте!).

Упражнение. 7 а) Квадрат нечетного числа дает остаток 1 не только при делении на 4, но даже при делении на 8. Докажите это. б) Решите в целых числах уравнение $x^2 + y^2 + z^2 = 8n - 1$. в) Никакое число вида $4^m(8n+7)$, где m, n – целые неотрицательные числа, не представимо в виде суммы квадратов трех целых чисел. Докажите это.

Произведение сумм квадратов

Мы уже нашли несколько признаков непредставимости числа в виде суммы двух квадратов. Не менее важны признаки представимости. Начнем с того, что если $n = x^2 + y^2$, то

$$(x+y)^2 + (x-y)^2 = x^2 + 2xy + y^2 + x^2 - 2xy + y^2 = 2\left(x^2 + y^2\right) = 2n.$$

Значит, вместе с каждым представимым числом n представимо и число $2n$. Далее,

$$(2x+y)^2 + (x-2y)^2 = 4x^2 + 4xy + y^2 + x^2 - 4xy + 4y^2 = 5\left(x^2 + y^2\right) = 5n.$$

Легко проверить и формулы

$$(2x+3y)^2 + (3x-2y)^2 = 13n,$$

$$(4x+y)^2 + (x-4y)^2 = 17n.$$

Все они являются частными случаями общей формулы, которая представляет произведение сумм двух квадратов в виде суммы двух квадратов. Чтобы получить ее, раскроем скобки

$$\left(a^2 + b^2\right)\left(x^2 + y^2\right) = a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2,$$

прибавим и отнимем $2abxy$ и изменим порядок слагаемых:

$$\left(a^2 + b^2\right)\left(x^2 + y^2\right) = a^2x^2 + 2axby + b^2y^2 + b^2x^2 - 2bxay + a^2y^2 = (ax+by)^2 + (bx-ay)^2. \quad (1)$$

Упражнение 8. Докажите, что

а) если четное число n есть сумма квадратов двух целых чисел, то и число $n/2$ представимо в виде суммы квадратов двух целых чисел;

б)* если кратное 5 число n есть сумма квадратов двух целых чисел, то число $n/5$ тоже представимо в таком виде;

в)* если $13k = x^2 + y^2$, где k, x, y – целые числа, то хотя бы одна из формул $k = \left(\frac{3x+2y}{13}\right)^2 + \left(\frac{2x-3y}{13}\right)^2$ и $k = \left(\frac{3x-2y}{13}\right)^2 + \left(\frac{2x+3y}{13}\right)^2$ представляет k в виде суммы квадратов целых чисел.

Теорема Ферма–Эйлера

Поскольку мы научились представлять произведение сумм двух квадратов в виде суммы двух квадратов, очень важно выяснить, какие простые числа представимы в виде суммы двух квадратов целых чисел, а какие не представимы. Числа вида $4n + 3$, как утверждает теорема 3, не представимы. Поэтому рассмотрим простые числа, которые при делении на 4 дают остаток 1. Это: $5 = 2^2 +$