Функция Кармайкла от степеней простых чисел такова: $\lambda(2) = 1$, $\lambda(4) = 2$, $\lambda(2^m) = 2^{m-2}$ при $m \geq 3$, $\lambda(p^m) = p^{m-1}(p-1)$ для любых нечетного простого p и натурального m.

Упражнение 27*. Докажите это, считая известным, что если p – нечетное простое, то для любого $k < p-1$ существует такое не кратное p число g, что $g^k \not\equiv 1 \pmod p$.

Следствия из малой теоремы Ферма

Теорема 3 позволяет легко решать многие задачи, которые без нее или очень трудны, или вообще недоступны. Рассмотрим букет таких задач, начав с одной из тех пяти, которые сформулированы в конце первой части статьи.

Простые делители чисел вида $a^4 + a^3 + a^2 + a + 1$

Если сумма $a^4 + a^3 + a^2 + a + 1$ кратна простому числу p, то число

$$a^5 - 1 = (a-1)\left(a^4 + a^3 + a^2 + a + 1\right)$$

тоже кратно p. Рассмотрим два случая.

Пусть $a \equiv 1 \pmod p$. Тогда $a^4 + a^3 + a^2 + a + 1 \equiv 1^4 + 1^3 + 1^2 + 1 + 1 = 5 \pmod p$, так что число p должно быть делителем числа 5. Попросту говоря, $p = 5$.

Пусть теперь $a \not\equiv 1 \pmod p$. Тогда порядок числа a по модулю p равен 5. Поскольку порядок является делителем числа $p-1$, то $p-1$ делится на 5.

Итак, *если простое число p является делителем числа вида $a^4 + a^3 + a^2 + a + 1$, то $p = 5$ или $p \equiv 1 \pmod 5$.*

Когда мы докажем теорему о существовании первообразного корня, то поймем, что верно и обратное утверждение. А именно, для $p = 5$ годится $a = 1$, а для простого числа $p = 5k + 1$ годится $a = g^k$, где g – первообразный корень по модулю p. В самом деле, $g^{5k} = g^{p-1} \equiv 1 \pmod p$. Следовательно, произведение $(a-1)\left(a^4 + a^3 + a^2 + a + 1\right) = a^5 - 1$ кратно p. Поскольку первый множитель не делится на p, второй должен делиться, что и требовалось доказать.

Упражнения

28 (М1324). Ни при каком целом a число $a^2 + a + 1$ не кратно а) 5; б) 11; в) 17; г) $6m - 1$, где m – натуральное число. Докажите это.

29. Докажите, что всякий положительный делитель числа $a^4 - a^2 + 1$ дает остаток 1 при делении на 12.

30. Докажите, что если порядок числа a по простому модулю p равен

а) 3, то число $a^2 + a + 1$;

б) 4, то число $a^2 + 1$;

в) 15, то число $a^8 - a^7 + a^5 - a^4 + a^3 - a + 1$

кратно p. (Тот, кто знаком с многочленами деления круга, скажет, что это упражнение – частный случай общего утверждения: число a имеет порядок k тогда и только тогда, когда k – делитель числа $p-1$ и $\Phi_k(a) \equiv 0 \pmod p$.)

31. Если по простому модулю p число a имеет порядок а) 3, то порядок числа $a + 1$ равен 6; б) 10, то порядок числа $a^3 - a^2 + a - 1$ равен 5. Докажите это.

32. а) Пусть a – натуральное число, $a > 1$, p – простое, $p > 2$. Докажите, что всякий простой делитель q числа $a^p \pm 1$ является делителем числа $a \pm 1$ или имеет вид $q = 2pm + 1$, где m – натуральное.

б) Пусть a, b – взаимно простые целые числа, n – натуральное, q – простое, $a^n - b^n$ делится на q, и пусть ни для одного отличного от n делителя m числа n разность $a^m - b^m$ не делится на q. Докажите, что $q \equiv 1 \pmod n$. (Биркгоф и Вандивер, используя свойства многочленов деления круга, доказали в 1902 году, что для любых (кроме одного исключительного случая, о котором сказано ниже) натуральных взаимно простых чисел a и b, где $a > b$, и для любого натурального числа $n > 2$ существует простой делитель q разности $a^n - b^n$, не являющийся делителем ни одной разности $a^m - b^m$, где $m < n$. Единственное исключение: $a = 2$, $b = 1$, $n = 6$.)

Простые делители чисел вида $a^{2^n} + 1$

Если $a^2 + 1$ делится на простое число p, $p \neq 2$, то

$$a^2 \equiv -1 \pmod p,$$

откуда

$$a^4 = \left(a^2\right)^2 \equiv (-1)^2 = 1 \pmod p.$$

Значит, порядок числа a равен одному из чисел 1, 2 и 4.

Первый и второй случаи невозможны, поскольку сравнение $a^2 \equiv 1$ противоречит сравнению $a^2 \equiv -1 \pmod p$.

В третьем случае в силу теоремы 3 имеем: $p - 1$ делится на 4. Мы доказали довольно общее и часто используемое утверждение: *любой нечетный простой делитель числа $a^2 + 1$ имеет вид $p = 4k + 1$ (а не $4k + 3$).*

Рассуждая аналогично, можно доказать, что если p – нечетный простой делитель числа $a^{2^n} + 1$, то $p - 1$ делится на 2^{n+1}.

Верно и обратное: для любого простого числа $p = 2^{n+1}k + 1$ существует кратное ему число вида $a^{2^n} + 1$. Доказать это очень легко, если знать теорему о существовании первообразного корня g. В самом деле, пусть $a = g^k$. Тогда

$$a^{2^n} = g^{2^n k} = g^{(p-1)/2}.$$

Число $g^{(p-1)/2}$ не сравнимо с единицей по модулю p, но квадрат этого числа есть $g^{p-1} \equiv 1 \pmod p$. Поэтому

$$a^{2^n} = g^{(p-1)/2} \equiv -1 \pmod p,$$

что и требовалось.

Упражнения

33. Если числа a и b взаимно просты, то всякий нечетный простой делитель p числа $a^{2^n} + b^{2^n}$ дает остаток 1 при делении на 2^{n+1}. Докажите это.

34. Пусть a, n – натуральные числа, причем a четно. Докажите, что числа n и $a^{2^n} + 1$ взаимно просты.

35. Пусть a, n – натуральные числа. Докажите, что

а) если $a^n + 1$ делится на $n + 1$, то a и n нечетны;

б) если a нечетно и $a > 1$, то существует бесконечно много натуральных n, для которых $a^n + 1$ делится на $n + 1$.

36. а) Пусть $n > 1$ и $2^n + 2$ делится на n. Докажите, что n четно.

б) Существует бесконечно много таких натуральных n, что $2^n + 2$ кратно n. Докажите это.

37 (Международная математическая олимпиада, 1996 г.). Пусть a, b – такие натуральные числа, что $15a + 16b$ и $16a - 15b$ – квадраты натуральных чисел. Найдите наименьшее возможное значение меньшего из этих квадратов.

Когда $2^n + 1$ делится на n?

Этот вопрос один из нас задал себе скорее в шутку, чем всерьез. И очень долго мы оба не понимали, что закономерности, обнаруживаемые в вычислениях, производимых следующей программой[8], имеют самое непосредственное отношение к малой теореме Ферма.

[8] *Программу для нас написал В.Иофик – тогда абитуриент, а сейчас – студент мехмата МГУ.*