Малая теорема Ферма

(См. «Квант» №4)

44. Если НОД$(s, p-1) = d > 1$, то $\left(g^s\right)^{(p-1)/d} = \left(g^{s/d}\right)^{p-1} \equiv 1 \pmod p$. Поскольку $(p-1)/d < p-1$, мы доказали, что число g^s не является первообразным корнем по модулю p. Осталось доказать, что если НОД$(s, p-1) = 1$, то g^s – первообразный корень. Это можно делать разными способами. Можно доказывать, что числа s, $2s$, $3s$, …, $(p-1)s$ дают разные остатки при делении на $p-1$ (попробуйте!). А можно рассуждать «от противного»: если бы g^s не было первообразным корнем, то существовало бы натуральное число $r < p-1$, для которого $\left(g^s\right)^r \equiv 1 \pmod p$; но тогда sr должно делиться на $p-1$, что невозможно из-за взаимной простоты чисел s и $p-1$.

46. а) 5; б) 6. в) Так как $257 = 2^8 + 1$, то $2^{16} - 1$ делится на 257. Следовательно, порядок числа 2 по модулю 257 не превосходит $16 < 256$. Проверим, что 3 – первообразный корень: $3^8 \equiv 136$, $3^{16} \equiv 249 \equiv -2^3$, $3^{64} \equiv 2^{12} = 1024 \cdot 4 \equiv (-4) \cdot 4 = -16$, следовательно, $3^{128} - 1 = \left(3^{64} - 1\right)\left(3^{64} + 1\right) \not\equiv 0 \pmod{257}$. *Ответ*: 3.

47. а) $2^8 \equiv -7 \pmod{263}$, $2^{16} \equiv 49$, $2^{32} \equiv 34$, $2^{64} \equiv 104$, $2^{128} \equiv 33$; следовательно, $2^{131} = 2^3 \cdot 2^{128} \equiv 8 \cdot 33 \equiv 1$. Значит, 2 не является первообразным корнем, а -2 – является: $(-2)^{131} \equiv -1 \not\equiv 1$ и $(-2)^2 \not\equiv 1 \pmod{263}$. б) *Указание*. Если $a^3 \not\equiv a$, то $a \not\equiv 0$ и $(\pm a)^2 \not\equiv 1$. Имеем $a^{82} - 1 = \left(a^{41} - 1\right)\left(a^{41} + 1\right)$. Значит, для всякого $a (\not\equiv 0)$ либо $a^{41} \equiv 1$, либо $a^{41} \equiv -1$. И вообще, для всякого простого числа $p = 2q + 1$, где q – тоже простое, $q > 2$, ровно одно из чисел a и $-a$, где $a^3 \not\equiv a \pmod p$, является первообразным корнем по модулю p.

50. а) $x \equiv 1$, $2^3 \equiv 8$, $2^6 \equiv 12$ или $2^9 \equiv 5 \pmod{13}$.

51. *Указание*. $x^7 - 1 = (x-1)\left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right)$. *Ответ*: $x \equiv 2^4$, 2^8, 2^{12}, 2^{16}, 2^{20} или $2^{24} \pmod{29}$. (Этот же ответ можно записать иначе: $x \equiv 16$, 24, 7, 25, 23 или 20.)

52. Если k делится на $p-1$, то все слагаемые сравнимы с 1 по модулю p и потому сумма сравнима с $p - 1 \not\equiv 0 \pmod p$. Если же k не делится на $p-1$, то существует такое не кратное p число x, что $x^k \not\equiv 1 \pmod p$. Обозначим $S = 1^k + 2^k + \ldots + (p-1)^k$. Сумма $x^k + (2x)^k + \ldots + \left((p-1)x\right)^k = x^k S$ сравнима с S по модулю p, поскольку (после взятия остатков от деления на p) ряд чисел x, $2x$, $3x$, …, $(p-1)x$ отличается от ряда 1, 2, …, $p-1$ только перестановкой, а от перемены мест слагаемых сумма не меняется. Значит, $x^k S \equiv S \pmod p$, откуда $\left(x^k - 1\right)S \equiv 0$, т.е. $S \equiv 0 \pmod p$.

Если пользоваться существованием первообразного корня, то доказывать, что при k, не кратных $p-1$, сумма S кратна p, можно и при помощи формулы суммы геометрической прогрессии:

$$1^k + g^k + g^{2k} + \ldots + g^{(p-2)k} = \frac{1 - g^{(p-1)k}}{1 - g^k} \equiv 0 \pmod p.$$

Ответ: при k, не кратных $p-1$.

53. а) $101^2\left(1 + 2 \cdot 8^2\right) = 1315929$; б) $17^3\left(1 + 6 \cdot 8^2\right) = 1891505$.

55. *Ответ*: $\varphi(n)/2$. *Указание*. Если НОД$(a, n) = 1$, то и НОД$(n-a, n) = 1$.

56. *Ответ*: 1. *Указание*. Для каждого из чисел $a = 1, 2, \ldots, p-1$ существует и единственно такое число b, что $ab \equiv 1 \pmod p$ и $1 \le b \le p-1$. Это число b является первообразным корнем тогда и только тогда, когда a – первообразный корень.

57. б) *Указание*. Пусть, для определенности, q – простой делитель числа m. Тогда $(ab)^{mn/q} = a^{mn/q} \cdot \left(b^n\right)^{m/q} \equiv a^{mn/q} \not\equiv 1 \pmod p$, ибо mn/q не кратно числу m.

Далее, при $p = 5$ порядки чисел 2 и 3 равны 4, а порядок произведения $2 \cdot 3 \equiv 1 \pmod 5$ равен 1.

59. а) *Указание*. $n-1$ кратно числу $2p$. *Замечание*. Все числа $n = \left(4^p - 1\right)/3$, где $p > 3$, – составные. При $p = 5$ получаем $n = 341$.

61. б) При $a = 0$ или 1 годится $n = 4$; при $a = -2$ – число $n = 6$; при $a = 2$ – указанное в пункте а) число $n = 161038$. Если $|a| > 2$, то годится $n = |a|$, если a четно, и $n = 2|a|$, если нечетно.

в) Можно считать, что $a > 1$. Пусть $a^n \equiv a \pmod n$, причем n четно, $n > 2$. Рассмотрим такое (существующее по теореме Биркгофа – Вандивера) простое число p, что $a^{n-1} - 1$ кратно p, но ни при каком $m < n-1$ разность $a^m - 1$ не кратна p. В силу упражнения 32, б) число $p-1$ делится на $n-1$. Следовательно, $p \ge n$; а так как n четно, то $p > n$.

Поскольку $np - 1 = n - 1 + n(p-1)$ делится на $n-1$, то $a^{np-1} - 1$ делится на $a^{n-1} - 1$. По малой теореме Ферма, $a^{np-1} = a^{n(p-1)} \cdot a^{n-1} \equiv 1 \pmod p$.

Следовательно, разность $a^{np} - a$ делится и на n, и на p, а потому и на np. Строя таким образом все новые и новые числа, мы доказываем утверждение задачи.

62. б) Нетрудно проверить, что $n = 65$ – наименьшее составное натуральное число, для которого $3^{n-1} \equiv 2^{n-1} \pmod n$.

в) Если пользоваться бесконечностью множества чисел Кармайкла, то достаточно рассмотреть $n = 3^k - 2^k$, где k – число Кармайкла, и применить утверждение пункта а).

Можно обойтись и без этого, рассмотрев $n = 3^{2^t} - 2^{2^t}$. Тогда числа $3^{2^t} - 1$ и 2^{2^t} кратны 2^t, так что опять применимо утверждение пункта а).

63. *Указание*. Для любого числа a, взаимно простого с n, рассмотрите сумму $S = a^{n-1} + (2a)^{n-1} + \ldots + \left((n-1)a\right)^{n-1}$. Докажите, что $S \equiv 1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1} \equiv -1$ и $S \equiv a^{n-1}\left(1^{n-1} + 2^{n-1} + \ldots + (n-1)^{n-1}\right) \equiv -a^{n-1} \pmod n$.

65. Если p – простой делитель составного числа n, то $C_n^p / n = (n-1)(n-2)\ldots(n-p+1)/p!$ – не целое число, поскольку делимое не кратно p.

66. а) $a + \dfrac{a^p - a}{p} + \dfrac{a^{p^2} - a^p}{p^2}$;

б) $a + \dfrac{a^p - a}{p} + \dfrac{a^q - a}{q} + \dfrac{a^{pq} - a^p - a^q + a}{pq}$.

.