казать очень коротко. В равенство

$$f(x) = (x-a)g(x) + r,$$

где $g(x)$ – многочлен (неполное частное), а r – число (остаток), можно подставить вместо x число a. Получим

$$f(a) = (a-a)g(a) + r = r.$$

Значит, остаток r от деления $f(x)$ на $x-a$ равен $f(a)$. Это и есть теорема Безу.

А для остальных читателей теорему Безу можно сформулировать и доказать чуть более длинным, но не менее естественным способом.

Теорема 5. *Число a является корнем многочлена $f(x)$ в том и только том случае, когда $f(x)$ делится на $x-a$, т.е. когда*

$$f(x) = (x-a)g(x),$$

где g – некоторый многочлен.

Доказательство. Если

$$f(x) = (x-a)g(x),$$

то

$$f(a) = (a-a)g(a) = 0.$$

Обратно, пусть $f(a) = 0$. Подставим в многочлен

$$f(x) = k_n x^n + k_{n-1}x^{n-1} + \ldots + k_2 x^2 + k_1 x + k_0$$

число a. Получим

$$0 = f(a) = k_n a^n + k_{n-1}a^{n-1} + \ldots + k_2 a^2 + k_1 a + k_0.$$

Следовательно,

$$f(x) = f(x) - f(a) = k_n\left(x^n - a^n\right) + k_{n-1}\left(x^{n-1} - a^{n-1}\right) + \ldots + k_2\left(x^2 - a^2\right) + k_1(x-a).$$

Каждая из разностей

$x - a$,

$x^2 - a^2 = (x-a)(x+a)$,

…

$x^n - a^n =$

$= (x-a)\left(x^{n-1} + x^{n-2}a + \ldots + xa^{n-2} + a^{n-1}\right)$

кратна $x-a$. Теорема доказана.

Переформулировка малой теоремы Ферма

Из теоремы Безу следует, что если a_1, a_2, …, a_m – различные корни многочлена $f(x)$, то $f(x) = (x-a_1)(x-a_2)\ldots(x-a_m)g(x)$, где g – некоторый многочлен.

Применив это соображение к многочлену $x^{p-1} - 1$, получим замечательную переформулировку малой теоремы Ферма:

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-p+1),$$

где знак сравнения означает, что если раскрыть все скобки в правой части и вычесть из нее левую, то получим многочлен, коэффициенты которого кратны p. Как вы помните, для частных случаев $p = 2, 3, 5, 7$ и 11 это разложение на множители встречалось в первой части статьи.

Упражнение 49. Подставив $x = 0$, докажите теорему Вильсона: $(p-1)! \equiv -1 \pmod p$ для любого простого числа p.

Сравнение $x^k \equiv 1 \pmod p$

Если k – делитель числа $p-1$, т.е. $p - 1 = km$, то

$$x^{p-1} - 1 = \left(x^k - 1\right)\left(x^{k(m-1)} + x^{k(m-2)} + \ldots + x^k + 1\right).$$

Значит, многочлен $x^k - 1$ является делителем многочлена $x^{p-1} - 1$. Поскольку $x^{p-1} - 1$ разлагается в произведение многочленов первой степени, то его делитель $x^k - 1$ является произведением k многочленов первой степени.

Немного подумав, можно сообразить, что мы доказали следующее утверждение.

Теорема 6. *Если p – простое число, k – делитель числа $p-1$, то сравнению $x^k \equiv 1 \pmod p$ удовлетворяют ровно k классов вычетов по модулю p.*

Упражнения

50. Решите сравнения

а) $x^4 \equiv 1 \pmod{13}$; б) $x^{1604} \equiv 1 \pmod{17}$. (*Указание.* 2 и 3 – первообразные корни, соответственно, по модулю 13 и по модулю 17.)

51. Зная, что 2 – первообразный корень по модулю 29, решите сравнение

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{29}.$$

52. Пусть p – простое число. При каких k сумма $1^k + 2^k + \ldots + (p-1)^k$ кратна p?

53. а) Сколько существует таких пар (a,b) натуральных чисел, что $a, b \le 1717$ и $a^8 + b^8$ кратно 17?

б) Сколько существует таких троек (a,b,c) натуральных чисел, что $a,b,c \le 289$ и $a^{1000} + b^{3000} + c^{9000}$ кратно 17?

Сумма значений функции Эйлера

Рассмотрим 100 дробей: $1/100$, $2/100$, …, $100/100$. Если каждую из них привести к несократимому виду, то получим $\varphi(100) = 40$ дробей со знаменателем 100, $\varphi(50) = 20$ дробей со знаменателем 50, и так далее: для каждого делителя d числа 100 получим $\varphi(d)$ дробей со знаменателем d. (Почему? Потому что $\varphi(d)$ – это количество несократимых правильных дробей со знаменателем d.)

Мы получили замечательное равенство:

$$100 = \varphi(100) + \varphi(50) + \varphi(25) + \varphi(20) + \varphi(10) + \varphi(5) + \varphi(4) + \varphi(2) + \varphi(1).$$ [2]

Если бы мы рассмотрели не дроби со знаменателем 100, а дроби со знаменателем n, то точно так же доказали бы следующее утверждение.

Теорема 7. *Для любого натурального числа n сумма значений функции Эйлера $\varphi(d)$ по всем делителям d числа n равна n.*

Упражнения

54. Если d – делитель числа n, то существует ровно $\varphi(n/d)$ таких натуральных чисел k, что $k \le n$ и $\text{НОД}(k,n) = d$. Докажите это.

55. Пусть $n > 1$. Найдите сумму всех несократимых правильных дробей, знаменатели которых равны n.

Доказательство теоремы 4

Мы должны доказать, что если k – делитель числа $p-1$, то среди ненулевых классов вычетов по простому модулю p существует ровно $\varphi(k)$ классов порядка k.

Применим индукцию. *База.* Для $k = 1$ утверждение верно.

Переход. Рассмотрим некоторый делитель k числа $p-1$. Предположим, что для любого делителя d числа k, где $d < k$, существует ровно $\varphi(d)$ классов вычетов порядка d. Найдем количество классов вычетов порядка k.

В силу теоремы 6, сравнению $x^k \equiv 1 \pmod p$ удовлетворяют ровно k классов вычетов. Каждое решение x этого сравнения имеет некоторый

[2] *Для Фомы неверующего: 40 + 20 + 20 + 8 + 4 + 4 + 2 + 1 + 1 = 100.*