Теорема Зигмонди

Гусев Антон Сергеевич

26 февраля 2020 г. — 27 февраля 2020 г.

Пусть нам даны числа $a > b$. Обозначим $d_n = a^n - b^n, s_n = a^n + b^n$.

Теорема 1 (Зигмонди −). Для любого n у d_n есть простой делитель, которого нет у d_k при $k < n$, кроме случаев

1. $n = 2, a + b = 2^l$. Тогда $2 \mid a - b$ и других делителей у $a + b$ нет.
2. $n = 6, a = 2, b = 1$. Тогда у 63 простые делители 3 (встречается при $n = 2$) и 7 ($n = 3$).

Теорема 2 (Зигмонди +). То же, что и 1, для s_n. Исключение — $n = 3, a = 2, b = 1$.

Обозначим $ord_p(x) = ord_{p_j}(p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}) = \alpha_j$.

Лемма 3 (об уточнении показателя). Пусть $a, b, n \in \mathbb{N}, p \in \mathbb{P}, p \mid a - b, p \nmid a, p \nmid b$. Тогда:

1. Если $p > 2$, то $ord_p(a^n - b^n) = ord_p(a - b) + ord_p(n)$.
2. Если $p = 2$, то это верно при условии, что $4 \mid a - b$.

Доказательство. Рассмотрим несколько случаев:

1. Пусть $p \nmid n$. Тогда $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$. Докажем, что вторая скобка не делится на p. Так как $a \equiv b \mod p$, то эта скобка сравнима с $a^{n-1}n$, но $p \nmid a, p \nmid n$.
2. Пусть $p = n$. Тогда ясно, что вторая скобка делится на p (там p слагаемых, каждое сравнимо с 1). Пусть $a - b = pk$. Если $p \mid k$, то это верно (аналогично предыдущему пункту). Значит, $p \nmid k$. Тогда пусть $k = px - m$. Значит,

$$a^{p-1} + a^{p-2}b + \ldots + b^{p-1} \equiv a^{p-1} + a^{p-2}(a + mp) + \ldots + (a + mp)^{p-1} \mod p^2.$$

   Посмотрим на $a^{p-1-t}(a+pm)^t \mod p^2$. В разложении этого по биному почти все слагаемые делятся на p^2, остаётся $a^{p-1}+a^{p-2}pmt$. Когда мы сложим все такие слагаемые, мы получим $pa^{p-1} + a^{p-2}pm\frac{p(p-1)}{2} \mod p^2$ и первое слагаемое не делится на p^2 при $p > 2$, а второе делится. Если же $p = 2$, то это тоже работает, потому что $m = 0$.

Завершение доказательства. Пусть $n = p^r s, p \nmid s$ и $r > 0$. Тогда

$$ord_p\left(a^n - b^n\right) = ord_p\left(\left(a^{p^{r-1}}s\right)^p - \left(b^{p^{r-1}}s\right)^p\right) = 1 + ord_p\left(a^{\frac{n}{p}} - b^{\frac{n}{p}}\right).$$

Индукция по r. ■

Многочлены деления круга

Рассмотрим $P(x) = x^n - 1$. Заметим, что корни этого многочлена — точки, которые делят единичную комплексную окружность на n равных частей. Рассмотрим такое α, что $(\cos\alpha + i\sin\alpha)^n = 1$. Тогда по формуле Муавра получается $\alpha = \frac{2\pi k}{n}$. Тогда если рассмотреть x_1 — корень с самым маленьким положительным аргументом, то получится $x_j = x_1^j$ для всех остальных корней. Можно записать $\xi_n = x_1$. Тогда обозначим **многочлен деления круга** —

$$\Phi_n(x) = \prod_{k=1;\ (k,n)=1}^{n} (x - \xi_n^k).$$

Примеры

- $\Phi_1(x) = x - 1$.
- $\Phi_2(x) = x - (-1) = x + 1$.
- $\Phi_3(x) = \frac{x^3-1}{x-1} = x^2 + x + 1$.
- $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$.

Лемма 4. $\varphi(n) = \sum_{d|n} \varphi(d)$.

Доказательство. Рассмотрим дроби $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$ и сократим их. Тогда для каждого $d \mid n$ дробей со знаменателем d будет $\varphi(d)$. ■

Лемма 5. $x^n - 1 = \prod_{d|n} \Phi_d(x)$.

Доказательство. Если мы докажем, что у них совпадают степень, старший коэффициент и корни, то мы докажем это. У обоих многочленов старший коэффициент 1 и степень n (потому что у Φ_m степень $\varphi(m)$). Набор корней $x^n - 1$ — это ξ_n^k для разных k. Заметим, что $\xi_n^k = \xi_{n/t}^{k/t}$. Тогда если взять $t = (n, k)$, то это число будет корнем $\Phi_{n/t}(x)$. ■

Лемма 6. У Φ_n целые коэффициенты.

Доказательство. Индукция по n.

База. $n = 1, 2$.

Переход $n \le k \to n = k+1$. По 5 мы знаем, что $x^{k+1} - 1 = \prod_{d|k+1} \Phi_d(x)$, то есть $\Phi_{k+1} = \frac{xk+1-1}{\prod \Phi_{\ldots}}$ и у знаменателя целые коэффициенты по предположению индукции. Заметим, что когда мы будем делить многочлен $\mathbb{Q}[x]$ на другой многочлен $\mathbb{Q}[x]$, получим $\mathbb{Q}[x]$ (если поделится нацело). Значит, у Φ_{k+1} рациональные коэффициенты. Теперь у нас $x^{k+1} - 1 = \Phi_{k+1}(x)g(x), g(x) \in \mathbb{Z}[x]$. Вынесем из произведения t — общий знаменатель всех коэффициентов Φ_{k+1}. Пусть $p \mid t$ и в обоих многочленах есть коэффициент, который не делится на p. Тогда рассмотрим минимальный такой коэффициент $a_i x^i$ и минимальный аналогичный коэффициент $b_j x^j$. Тогда коэффициент при x^{i+j} должен делиться на p, но он не делится — противоречие. В $g(x)$ есть такой коэффициент (потому что старший член 1), значит, все коэффициенты Φ_{k+1} делятся на p. Значит, на самом деле $\Phi_{k+1} \in \mathbb{Z}[x]$. ■

Лемма 7 (Критерий Эйзенштейна). Пусть у $P(x)$ все коэффициенты, кроме старшего, кратны p, и свободный член не делится на p^2. Тогда $P(x)$ неприводим над $\mathbb{Q}$.

Доказательство. Пусть $P(x) = \sum a_i x^i = \left(\sum b_j x^j\right)\left(\sum c_k x^k\right)$. Ровно один из коэффициентов b_0 и c_0 делится на p. Пусть $p \mid b_0$. Заметим, что $p \nmid b_m$, значит, можно рассмотреть минимальное такое i, что b_i не кратно p. Тогда коэффициент при x^i у $P(x)$ не может делиться на p — противоречие. ■

Лемма 8. $\Phi_p(x)$ неприводим над $\mathbb{Q}$.

Доказательство. $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1$. Подставим $x = y + 1$. Тогда у получившегося многочлена свободный член будет равен p, а все остальные, кроме старшего, кратны p, что противоречит 7. ■

Лемма 9. Пусть $n \in \mathbb{N}, p \in \mathbb{P}$. Тогда

$$\Phi_{np}(x) = \begin{cases} \Phi_n(x^p), p \mid n \\ \dfrac{\Phi_n(x^p)}{\Phi_n(x)}, p \nmid n \end{cases}$$

Доказательство. Пусть $p \mid n$. Тогда у этих многочленов одинаковый старший член 1 и одинаковая степень $\varphi(np)$. Посмотрим на их корни. У первого многочлена это точки, делящие окружность на np частей, но не на меньшее количество, а у второго те же самые точки.

Теперь пусть $p \nmid n$. Старший коэффициент у них снова 1. Степень $\Phi_{np}(x)$ равна $\varphi(n)(p-1)$, степень $\Phi_n(x^p)$ равна $p\varphi(n)$, степень $\Phi_n(x)$ равна $\varphi(n)$. Докажем про корни. Корни $\Phi_{np}(x)$ — те точки, номера которых взаимно просты с np, а корни Φ_n — те, которые взаимно просты с n и делятся на p. Тогда у произведения корни — все точки, номера которых взаимно просты с n. ■

Пример использования леммы. Лемма позволяет посчитать любое Φ_n через Φ_p:

$$\Phi_{12}(x) = \Phi_6(x^2) = \frac{\Phi_3(x^4)}{\Phi_3(x^2)} = \frac{x^8 + x^4 + 1}{x^4 + x^2 + 1}.$$

Лемма 10. Пусть $k \mid n$. Тогда $\Phi_n(a)(a^k - 1) \mid a^n - 1$.

Доказательство.

$$a^n - 1 = \prod_{d|n} \Phi_d(a) = \Phi_n(a) \cdot \prod_{d|n, d<n} \Phi_d(a),$$

причём в правом произведении есть множитель $a^k - 1$. ■

Теорема 11 (Упрощение Зигмонди). Пусть $b = 1$. Тогда для любого n у d_n есть простой делитель, которого нет у d_k при $k < n$, кроме тех же двух исключений.

Лемма 12. Если 11 неверна, то $p \mid \Phi_n(a) \implies p \mid n$.

Доказательство. $p \mid \Phi_n(a) \implies p \mid a^n - 1$. Тогда если теорема 11 неверна, то $p \mid a^k - 1$ для какого-то $k < n$. Тогда по алгоритму Евклида можно получить, что $p \mid a^m - 1$ для какого-то $m \mid n$. Применим 10. Тогда $p(a^k - 1) \mid a^n - 1$. Тогда если $p > 2$ или $4 \mid a^k - 1$, то по 3 мы получим

$$ord_p(a^n - 1) = ord_p(a^k - 1) + ord_p\left(\frac{n}{k}\right) \implies p \mid \frac{n}{k} \implies p \mid n,$$

что и требовалось. Пусть $p = 2$ и $a^k - 1$ не делится на 4. Кроме того, $2 \mid a^n - 1 \implies k = 1$. Тогда если 3 не работает, то $4 \nmid a - 1$. Значит, $a = 4k + 3$. Пусть $2 \nmid n$. Тогда $ord_2(a^n - 1) = ord_2(a^k - 1)$, противоречие с 10. ■

Лемма 13. $\Phi_n(a)$ свободно от квадратов.

Доказательство. Докажем, что $p^2 \nmid \Phi_n(a)$. Пусть $n = p^\alpha s$. Тогда $\Phi_n(a) \cdot \left(a^{p^{\alpha-1}s} - 1\right) \mid a^{p^\alpha s} - 1$. Заметим, что $t \mid s$, где t — показатель $a \mod p$. Тогда знаменатель кратен p. Применим 3. Получим, что степень вхождения p в $(a^{n/p} - 1)/(a^n - 1)$ равен 1, кроме случая $p = 2$. ■

Лемма 14. Пусть $p \mid \Phi_n(a)$ и $n = p^\alpha s$. Тогда s — показатель a по p.

Доказательство. Пусть T — показатель. Тогда

$$p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{p^\alpha T} - 1} \text{ и } 1 \leq ord\left(\frac{a^{p^\alpha s} - 1}{a^{p^\alpha T} - 1}\right) = ord\left(\frac{a^s - 1}{a^T - 1}\right) = 0. ■$$

Доказательство теоремы 11. Заметим, что по 14 если $p \mid F_n(a)$, то p — самый большой простой делитель в n. Значит, простых делителей максимум 1. Тогда по 13 $F_n(a) = p$. С другой стороны, $\Phi_n(a) = \Phi_{p^\alpha s}(a)$. Рассмотрим несколько случаев:

1. Пусть $\alpha > 1$. Тогда $\Phi_n(a) = \Phi_{n/p}(a^p) \geq a^p - 1 > p$. Такого не бывает.
2. Пусть $\alpha = 1, a \neq 2$. Тогда $\Phi_{ps} \geq (a-1)^{\varphi(ps)} \geq 2^{p-1}$.
3. Пусть $\alpha = 1, a = 2$. Тогда $\Phi_{ps}(2) = \frac{\Phi_s(2^p)}{\Phi_s(2)} \geq \frac{(2^p-1)^{\varphi(s)}}{3^{\varphi(s)}}$. Если $p > 3$, то такого не бывает. Если $p = 3$, то либо $n = 3$, либо $n = 6$. Если $p = 2$, то $n = 2$.

Итак, мы доказали, что у $\Phi_n(a)$ есть «уникальный» простой делитель p. Тогда $p \mid a^n - 1$ и если $p \mid a^k - 1$, то $p \mid \Phi_y(a)$ для какого-то y — противоречие. ■

Доказательство теоремы 1 (идея). Обозначим $\Phi_n(a, b) = \left(\frac{b}{a}\right)^{\varphi(n)} \Phi_n(a)$. Дальше надо те же самые рассуждения провести для $\Phi_n(a, b)$. ■

Доказательство теоремы 2 через 1. Очевидно следует из того, что $a^k + b^k \mid a^{2k} - b^{2k}$. ■