Теорема Зигмонди

Теорема Зигмонди. Для любых натуральных чисел $a, n > 1$ существует простое p такое, что показатель числа a по модулю p равен n, за исключением следующих ситуаций:

- $n = 2, a = 2^s - 1$, где $s \geqslant 2$;
- $n = 6, a = 2$.

Обобщенная теорема Зигмонди. 1. Для любых взаимно простых натуральных чисел $a > b \geqslant 1$ и любого натурального $n > 1$ существует простое p такое, что $a^n - b^n$ делится на p и при всех натуральных $k < n$ число $a^k - b^k$ не делится на p. Исключения составляют:

- $n = 2, a + b = 2^s$, где $s \geqslant 2$;
- $n = 6, a = 2, b = 1$.

2. Для любых взаимно простых натуральных чисел $a > b \geqslant 1$ и любого натурального $n > 1$ существует простое p такое, что $a^n + b^n$ делится на p и при всех натуральных $k < n$ число $a^k + b^k$ не делится на p. Исключение:

- $n = 3, a = 2, b = 1$.

1. Докажите, что последовательность $a_n = 3^n - 2^n$ не содержит геометрической прогрессии длины 3 в качестве подпоследовательности.

2. Найдите все решения $a, b \in \mathbb{N}$, $m \in \mathbb{Z}$ уравнения $2^a + m^b = 19^a$.

3. Решите уравнение $p^x - y^p = 1$ в натуральных числах, если p — простое.

4. Докажите, что у числа $2^{2^n} + 2^{2^{n-1}} + 1$ есть по крайней мере n различных простых делителей.

5. Пусть $2 < p < q$ — простые числа. Докажите, что у числа $2^{pq} - 1$ есть по крайней мере 3 различных простых делителя.

6. Докажите, что у $2^{p_1 p_2 \cdots p_n} + 1$ есть по крайней мере $2^{2^{n-1}}$ различных делителей. $p_1, p_2, \ldots, p_n$ — различные нечетные простые.

7. Найдите все тройки чисел a, m, n $(m, n > 1)$, что $(a + 1)^n$ делится на $a^m + 1$.

8. Решите уравнение $5^x - 3^y = z^2$ в натуральных числах.

Перед тем, как перейти к доказательству теоремы Зигмонди, напомним необходимые факты из жизни многочленов деления круга.

1. Если простое p не делит n, то $\Phi_n(a)$ кратно $p \iff$ показатель a по модулю p равен n. В частности, $p-1$ делится на n в этом случае.
2. Пусть p — простое. Тогда если n кратно p, то $\Phi_{np}(x) = \Phi_n(x^p)$; если же n не кратно p, то $\Phi_{np}(x) = \dfrac{\Phi_n(x^p)}{\Phi_n(x)}$.

9. *(Недостающие свойства круговых многочленов)*
(a) Пусть $n = p^t \cdot m$, где p — простое, m — не кратное p натуральное число, t — натуральное. Докажите, что

$$\Phi_n(x) = \frac{\Phi_m(x^{p^t})}{\Phi_m(x^{p^{t-1}})}.$$

(b) Даны простое p и натуральное a, не кратное p. Пусть θ — показатель a по модулю p. Докажите, что если для некоторого натурального n число $\Phi_n(a)$ делится на p, то $n = \theta \cdot p^t$, где t — целое неотрицательное.
(c) Для натуральных b, m получите оценки $(b-1)^{\varphi(m)} \leqslant \Phi_m(b) \leqslant (b+1)^{\varphi(m)}$.
(d) В условиях пункта (a) с помощью пункта (c) получите оценку

$$\Phi_n(a) \geqslant \left(\frac{b^p - 1}{b+1}\right)^{\varphi(m)},$$

где a — натуральное число, а за b обозначено $a^{p^{t-1}}$.

10. *(Доказательство теоремы Зигмонди)* Согласно факту 1 из жизни многочленов деления круга, достаточно показать, что у числа $\Phi_n(a)$ существует простой делитель p, не делящий n. Далее во всех пунктах предполагаем противное: любой простой делитель p числа $\Phi_n(a)$ входит также в n. Наша цель — привести это предположение к противоречию. Заметим сразу, что $(a, p) = 1$, поскольку $\Phi_n(a)$ делится на p и имеет свободный коэффициент 1. Пусть θ — показатель a по модулю p.
(a) Докажите, что $n = \theta \cdot p^t$ для некоторого натурального $t \geqslant 1$.
(b) Докажите, что $\Phi_n(a)$ не может иметь двух различных простых делителей.
(c) Докажите, что если $p \neq 2$, то p входит в $\Phi_n(a)$ в степени 1 (подсказка: используйте лемму об уточнении показателя для выражения $a^n - 1$).
(d) Докажите, что если $p = 2$, то либо оно входит в $\Phi_n(a)$ в степени 1, либо $n = 2$.

11. *(Завершение доказательства теоремы Зигмонди)* В предыдущей задаче показано, что в предположении противного $\Phi_n(a) = p$, где p — простое, либо $n = 2$. Сопоставьте это с оценкой из задачи 9d и завершите доказательство теоремы Зигмонди.

12. Выведите из теоремы Зигмонди её обобщённые версии.