Круговые многочлены

Напоминание. *Корнями n-ой степени из единицы* называются комплексные корни многочлена $x^n - 1$. В тригонометрической записи они имеют вид $\varepsilon_k = cos(\frac{2\pi k}{n}) + i\,sin(\frac{2\pi k}{n})$, $1 \leqslant k \leqslant n$. *Первообразным корнем степени n из единицы* будем называть корень если n — наименьшая степень в которой он даёт 1, т.е. ε_k, где $(k, n) = 1$.

Определение. Круговым многочленом порядка n называется многочлен

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \varepsilon_k)$$

0. **(а)** Чему равна степень $\Phi_n(x)$?
(б) Выпишите в явном виде многочлены $\Phi_1(x), \Phi_2(x), \Phi_3(x), \Phi_4(x), \Phi_p(x)$, где p — простое.

1. **(а)** Докажите, что $x^n - 1 = \prod_{n \,\vdots\, d} \Phi_d(x)$, где произведение берётся по всем натуральным делителям d числа n.
(б) Докажите, что $\Phi_n(x)$ — многочлен с целыми коэффициентами.

2. Найдите чему равно $\Phi_n(0)$ и $\Phi_n(1)$.

3. Пусть n — натуральное, p — простое.
(а) Докажите, что если $n \,\vdots\, p$, то $\Phi_{np}(x) = \Phi_n(x^p)$.
(б) Докажите, что если $(n, p) = 1$, то $\Phi_{np}(x) = \frac{\Phi_n(x^p)}{\Phi_n(x)}$.
(в) Докажите, что если n — нечётно, то $\Phi_{2n}(x) = \Phi_n(-x)$.
(г) Пусть a — натуральное, причём $(a, n) = 1$. Докажите, что $\Phi_n(x^a) = \prod_{a \,\vdots\, d} \Phi_{nd}(x)$.

4. Докажите, что все числа

$$10001, 100010001, 1000100010001, \ldots$$

являются составными.

5. Докажите, что число $2^{2^n} + 2^{2^{n-1}} + 1$ содержит в разложении на простые множители как минимум n простых чисел (возможно, совпадающих).

Важная лемма. Пусть n — натуральное, a — целое, p — простое, $(n, p) = 1$. Тогда $\Phi_n(a) \,\vdots\, p$ тогда и только тогда, когда a принадлежит показателю n по модулю p.

6. Цель этой задачи — доказать важную лемму.
(а) Докажите, что если d — показатель a по модулю p, то $\Phi_d(a) \,\vdots\, p$.
(б) Докажите, что если степень вхождения p в $a^n - 1$ больше, чем в $a^d - 1$, то $\frac{n}{d} \,\vdots\, p$.
(в) Докажите лемму.

7. Рассмотрите многочлен $\Phi_{p-1}(x)$ и поймите, что по модулю p существует первообразный корень.

8. **(Частный случай теоремы Дирихле).** Рассмотрев многочлен $\Phi_n(x)$ докажите, что для каждого натурального n существует бесконечно много простых чисел вида $kn + 1$.

9. Пусть m, n — натуральные, a — целое. Пусть $(\Phi_m(a), \Phi_n(a)) = d > 1$.
(а) Докажите, что m/n — степень некоторого простого p.
(б) Докажите, что d — степень того же простого p.

10. Докажите, что у числа в задаче 5 имеется как минимум n *различных* простых делителей.

11. Пусть $p_1, p_2, \ldots, p_n$ — различные нечётные простые. Докажите, что число $2^{p_1 p_2 \cdots p_n} + 1$ имеет как минимум $2^{2^{n-1}}$ делителей.