МНОГОЧЛЕНЫ ДЕЛЕНИЯ КРУГА.

1 порция. Неприводимые многочлены. Производная.

Определение. $\mathbb{Z}_p$ — множество всех остатков по модулю p.

Определение. $\mathbb{Z}[x]$ — множество всех многочленов с коэффициентами из $\mathbb{Z}$. $\mathbb{Q}[x]$ — множество всех многочленов с коэффициентами из $\mathbb{Q}$. $\mathbb{Z}_p[x]$ — множество всех многочленов с коэффициентами из $\mathbb{Z}_p$.

Многочлен $f(x) \in \mathbb{Q}[x]$ (или $\mathbb{Z}[x], \mathbb{Z}_p[x]$) делится на многочлен $g(x) \in \mathbb{Q}[x]$ (или $\mathbb{Z}[x], \mathbb{Z}_p[x]$), если существует такой многочлен $h(x) \in \mathbb{Q}[x]$ (или $\mathbb{Z}[x], \mathbb{Z}_p[x]$), что $f(x) = g(x)h(x)$.

Определение. Многочлен $f(x) \in \mathbb{Z}[x]$ (или $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$) *неприводим* над $\mathbb{Z}$ (или над $\mathbb{Q}$, $\mathbb{Z}_p$), если его нельзя представить в виде произведения двух многочленов из $\mathbb{Z}[x]$ (или из $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$), не являющихся константой.

Определение. Для многочлена $P(x) = \sum\limits_{k=0}^{n} a_k x^k$ определим многочлен, который будем назвать производной многочлена $P(x)$, следующим образом:

$$P'(x) = \sum_{k=1}^{n} a_k k x^{k-1}.$$

Задачи. Теория.

1. (лемма Гаусса) $c(h(x))$ — НОД коэффициентов многочлена $h(x) \in \mathbb{Z}[x]$. Пусть $f(x)$, $g(x) \in \mathbb{Z}[x]$. Докажите, что $c(f(x)g(x)) = c(f(x)) \cdot c(g(x))$.

2. Докажите, что многочлен $f(x) \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$.

3. (критерий Эйзенштейна) Докажите, что многочлен $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ неприводим, если $a_0, a_1, \ldots, a_{n-1}$ кратны p, но a_n не делится на p, а a_0 не делится на p^2.

4. Докажите, что $(f(x) + g(x))' = f'(x) + g'(x)$.

5. Докажите, что $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

6. Дан многочлен $P(x)$. Докажите, что существует такой многочлен $m(x)$, что $m(x)^2 | P(x)$ тогда и только тогда, когда $(P(x), P'(x)) \neq 1$.

Задачи. Практика.

7. Пользуясь критерий Эйзенштейна докажите, что многочлен $x^{p-1} + \cdots + x + 1$ неприводим.

8. У многочлена $x^n - 1 \in \mathbb{Z}[x]$ (или $\mathbb{Z}_p[x]$, $p \mid n$) все корни кратности один.

2 порция. Многочлены деления круга. Введение.

Обозначим через

$$\zeta_k = \cos\frac{2\pi}{k} + i\sin\frac{2\pi}{k} = e^{2\pi i/k}.$$

Определения. *Примитивным корнем из* 1 *степени* n будем называть такой корень уравнения $x^n - 1 = 0$, что он не является корнем уравнения $x^k - 1 = 0$ при $1 \leqslant k < n$.

Несложно убедиться, что примитивными корнями из 1 являются числа ζ_n^k, где $(k, n) = 1$ и $1 \leqslant k \leqslant n$.

Определения. *Многочленом деления круга (или круговым многочленом)* будем называть многочлен

$$\Psi_n(x) = \prod_{\substack{1\leqslant k\leqslant n\\(k,n)=1}} (x - \zeta_n^k).$$

Примеры.

$$\Psi_1(x) = x - 1,\ \Psi_2(x) = x + 1,\ \Psi_3(x) = x^2 + x + 1.$$

Задачи. Теория.

9. Докажите, что

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

10. Докажите, что $\Psi_n(x) \in \mathbb{Z}[x]$.

11. $p \in \mathbb{P}$. Докажите, что $\Psi_p(x)$ неприводим.

12. Докажите, что если $(a, n) = 1$, то

$$\Psi_n(x^a) = \prod_{d|a} \Psi_{nd}(x).$$

Задачи. Практика.

13. Найдите $\Psi_n(x)$ при $n = 4, \ldots, 10$.

14. Пусть $n \in \mathbb{N}$. Докажите, что число $2^{2^n} + 2^{2^{n-1}} + 1$ может быть представлено в в виде произведения по меньшей мере n простых чисел (не обязательно различных).

3 порция. Многочлены деления круга. Основные свойства.

Определение. $\varphi(n)$ — функция Эйлера, которая определяется для любого натурального n следующим образом

$$\varphi(n) = \#\{k \in \mathbb{N} : 1 \leqslant k \leqslant n, (k,n) = 1\}.$$

Определение. $\mu(n)$ — функция Мебиуса, которая определяется для любого натурального n следующим образом

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1, \\ (-1)^k, \text{ если } n = p_1 \dots p_k, \text{ где } p_1, \dots, p_k \text{ различные простые}, \\ 0, \text{ если } p^2 | n. \end{cases}$$

Задачи. Теория.

15. Докажите, что $\deg \Psi_n(x) = \varphi(n)$.

16. Докажите, что

$$\sum_{d|n} \mu(d) = \begin{cases} 0, \text{ если } n > 1, \\ 1, \text{ если } n = 1. \end{cases}$$

17. Докажите, что

$$\Psi_{np}(x) = \begin{cases} \Psi_n(x^p), & \text{если } p|n, \\ \frac{\Psi_n(x^p)}{\Psi_n(x)}, & \text{если } p \nmid n. \end{cases}$$

18. Докажите, что для нечетного $n > 1$ верно

$$\Psi_{2n}(x) = \Psi_n(-x).$$

19. Докажите, что

$$\Psi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

20. Докажите, что если

$$\Psi_n(x) = \sum_{k=0}^{\varphi(n)} a_k x^k,$$

то $a_k = a_{\varphi(n)-k}$.

Задачи. Практика.

21. Докажите, что нет простых чисел в последовательности

$$10001, 100010001, 1000100010001, \dots.$$

22. Докажите, что все коэффициенты многочленов $\Psi_n(x)$, где $n < 105$, равны 0, 1 или -1.

4 порция. Многочлены деления круга. Показатель числа.

Определение. Показателем числа a, $(a,p)=1$, по модулю p называется наименьшее натуральное k, что число a^k-1 делится на p.

Задачи. Теория.

23. Пусть $m \neq n \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid mn$. Тогда $(\Psi_m(x), \Psi_n(x)) = 1$ над $\mathbb{Z}_p$.

24. Пусть $m, n \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid mn$. Тогда невозможно следующее: $p \mid \Psi_m(a)$, $p \mid \Psi_n(a)$ для некоторого $a \in \mathbb{Z}$.

25. $p \in \mathbb{P}$. Докажите, что для любых a, $n \in \mathbb{Z}$, $n > 0$, $(p,n)=1$, выполняется $p \mid \Psi_n(a)$ тогда и только тогда, когда показатель числа a по модулю p равен n.

Задачи. Практика.

26. Докажите, что если $p \nmid n$ и существует натуральное a, что $p \mid \Psi_n(a)$, тогда $p-1$ делится на n.

27. Докажите, что для любого многочлена с целыми коэффициентами $P(x)$ существует бесконечное много таких простых p, что найдется целое число a, $p \mid P(a)$.

28. Выведите из предыдущих задач, что существует бесконечно много простых, сравнимых с 1 по модулю n.

5 порция. Многочлены деления круга. Теорема Зигмонди.

Здесь пригодятся большая часть знаний из прошлых порций! А также малая теорема Ферма: число $a^p - a$ делится на p.

Задачи. Теория.

29. Пусть $m \neq n \in \mathbb{N}$, $k \in \mathbb{Z}$. Известно, что

$$(\Psi_m(k), \Psi_n(k)) \neq 1.$$

Докажите, что тогда этот НОД есть степень некоторого простого числа p и $m/n = p^z$ для некоторого целого z.

Мы хотим доказать теорему ("почти теорему Зигмонди"):
Пусть даны натуральные числа $n > 1$, $a > 1$. Тогда существует такое простое число p, что $a^n - 1$ кратно p, а $a^k - 1$ не делится на p, если $1 \leqslant k < n$. Исключение составляют следующие ситуации:
1. $n = 2$, $a = 2^m - 1$, где $m > 1$,
2. $n = 6$, $a = 2$.

Дальше пригодится Lifting the Exponent Lemma в следующей форме:
Пусть для нечетного простого p верно $p \mid a^n - 1$. Тогда $\nu_p(a^{np} - 1) = \nu_p(a^n - 1) + 1$.

Задачи. Практика.

30. Докажите LTE в указанной форме.

31. Пусть $a, n > 1$. Предположим, что все простые делители $\Psi_n(a)$ являются делителями n. Докажите, что число $\Psi_n(a)$ — простое, на которое делится n, или $n = 2$.

32. Пусть $a, n > 1$. $n = p^k r$, где $p \nmid r$. Тогда выполяется неравенство

$$\Psi_n(a) > (b^{p-2}(b-1))^{\varphi(r)},$$

где $b = a^{p^{k-1}}$.

33. Завершите доказательство "почти теоремы Зигмонди".

6 порция. Применение теоремы Зигмонди.

Задачи. Практика.

34. Найдите все пятерки натуральных чисел (a, n, p, q, r):

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1).$$

35. Пусть $p_1, \ldots, p_n$ различные нечетные простые. Тогда у $2^{p_1 \cdots p_n} + 1$ имеется $2^{2^{n-1}}$ различных делителей.

36. Решите уравнение в натуральных числах $(l > 1)$

$$(1 + m^n)^l = (1 + m^k).$$

37. Используя многочлены деления круга в точках (b/a) докажите теорему Зигмонди в общем виде.
1. Даны натуральные числа a, b, n, такие, что $a > b$, $(a, b) = 1$, $n > 1$. Тогда существует такое простое число p, что $a^n - b^n$ делится на p, а $a^k - b^k$ не делится на p, если $1 \leqslant k < n$. Исключение составляют следующие ситуации:
a. $n = 2$, $a + b = 2^m$, где $m > 1$,
b. $n = 6$, $a = 2$.

2. Даны натуральные числа a, b, n, такие, что $a > b$, $(a, b) = 1$, $n > 1$. Тогда существует такое простое число p, что $a^n + b^n$ делится на p, а $a^k + b^k$ не делится на p, если $1 \leqslant k < n$. Исключение составляет следующая ситуация:
a. $n = 3$, $a = 2$, $b = 1$.

7 порция. Многочлены деления круга. Неприводимость.

Пришла пора использовать все накопившиеся знания о многочленах деления круга.

Задачи. Практика.

38. Пусть $f(x)$ минимальный многочлен ζ_n над $\mathbb{Z}$. Пусть $p \in \mathbb{P}$, $p \nmid n$. Докажите, что $f(x) \mid f(x^p)$ в $\mathbb{Z}[x]$. Подсказка: $\Psi_n(x) = f(x)g(x)$.

39. Докажите, что $\Psi_n(x) = f(x)$.

40. Докажите, что если $\Psi_p(x) = f(x)g(x)$, где $f(x), g(x) \in \mathbb{R}[x]$, коэффициенты $f(x)$ и $g(x)$ неотрицательны, а старшие коэффициенты равны 1, то все коэффициенты $f(x), g(x)$ равны 0 и 1.

41. Докажите, что не существует $f(x), g(x) \in \mathbb{R}[x]$, коэффициенты $f(x)$ и $g(x)$ неотрицательны, $\Psi_p(x) = f(x)g(x)$.

42. Пусть

$$1 + x + x^2 + \cdots + x^{n-1} = F(x)G(x),\ n > 1,\ F(x),\ G(x) \in \mathbb{Z}[x].$$

а) Докажите, что все коэффициенты этих многочленов нули и единицы.
б) Докажите, что один из многочленов $F(x)$ или $G(x)$ представим в виде $(1 + x + \cdots + x^{k-1})T(x)$, где $k > 1$, а коэффициенты $T(x)$ — нули и единицы.