Круговые многочлены

Корни степени n из 1

$\sqrt[n]{1}$, $z^n = 1$, $z_0 = 1, z_1, \dots, z_{n-1}$

$$e^z = e^{x+iy} = e^x(\cos y + i\sin y)$$

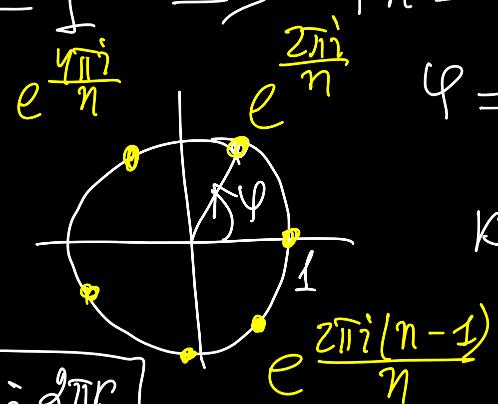
$x, y \in \mathbb{R}$

$$|z|^n = 1 \Rightarrow |z| = 1$$

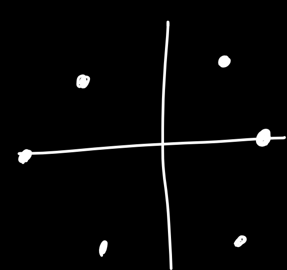
$$e^{i\varphi n} = 1 \Rightarrow \varphi n = 2\pi k$$

$$\varphi = \frac{2\pi k}{n}$$

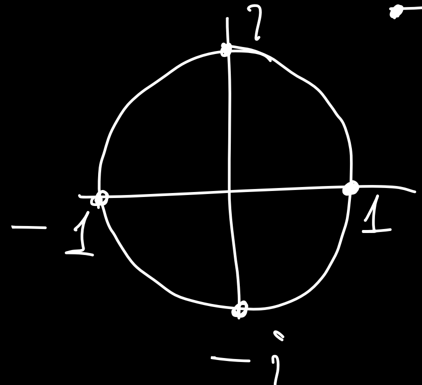
$e^{i\varphi}$



$k = 0, \dots, n-1$



$$\boxed{z = e^{i\frac{2\pi k}{n}}}$$



Опр. Примитивный корень из 1:

$e^{i\frac{2\pi k}{n}}$, где $(k,n)=1$

$e^{\frac{2\pi i}{n}}$

Утв. Примитивный корень n-й степени из 1 является образующей циклической группы $\{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \dots, e^{\frac{2\pi i(n-1)}{n}}\}$

$\triangleright$ $\langle e^{\frac{2\pi i k}{n}} \rangle = \{1, e^{\frac{2\pi i}{n}}, \dots, e^{\frac{2\pi i(n-1)}{n}}\}$

$$e^{\frac{2\pi i k a}{n}} = e^{\frac{2\pi i k b}{n}} \qquad a>b,\ a,b<n$$

$$\cancel{e^{\frac{2\pi k b}{n}}} \underbrace{\left(e^{\frac{2\pi i k(a-b)}{n}} - 1\right)}_{0} = 0$$

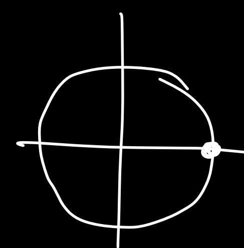
$$k(a-b) \,\vdots\, n \Rightarrow a-b \,\vdots\, n$$

$\triangleleft$

$$\sqrt[5]{1} \rightsquigarrow e^{\frac{2\pi i k}{5}}$$

<u>Опр.</u> $\Phi_n(x) = \prod\limits_{\substack{0<k<n \\ (k,n)=1}} \left(x - e^{\frac{2\pi i k}{n}}\right)$ — круговой многочлен

$$\prod_{0\le k\le n-1}\left(x-e^{\frac{2\pi i k}{n}}\right) = x^n - 1$$



Примеры: $\Phi_1(x) = x - e^{2\pi i} = x-1$

$$\Phi_2(x) = x - e^{\frac{2\pi i\cdot 1}{2}} = x+1$$

$$\Phi_3(x) = \prod(x-\xi) = \frac{\overbrace{\prod(x-\xi)}^{= x^3-1}}{x-1} =$$

ξ — любой корень степени 3

$1, \underline{e^{\frac{2\pi i}{3}}}, \underline{e^{\frac{4\pi i}{3}}}$ ξ — прим. кор. степени 3

$$= x^2+x+1$$

$$\Phi_4(x) = (x-i)(x+i) = x^2+1$$

$e^{\frac{\pi i}{2}} = i$, $e^{\frac{3\pi i}{2}} = -i$ $e^{\frac{2\pi i k}{4}}$

$$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$$

$$e^{\frac{2\pi i k}{5}},\quad e^{\frac{2\pi i}{5}},\ e^{\frac{4\pi i}{5}},\ e^{\frac{6\pi i}{5}},\ e^{\frac{8\pi i}{5}},\ \cancel{1} = e^{\frac{2\pi i\cdot 5}{5}}$$

Утв. $\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1}+\ldots+1$

Пример: $\Phi_{105}(x)$ – у него не все коэф-ты равны ± 1

Вопрос: Какова $\deg \Phi_n$?

Кол-во примитивных корней n-й степени

Их $\varphi(n)$, где φ – функция Эйлера

← количество таких $m<n$, что $(m,n)=1$

Утв. Круговой мн-н $\Phi_n(x)$ имеет целые коэф-ты

▷ $$\prod_{d|n} \Phi_d(x) = \underbrace{x^n-1}_{\prod\left(x-e^{\frac{2\pi i k}{n}}\right)}$$

$$\left.\begin{array}{l} A\subseteq B \\ B\subseteq A\end{array}\right\} \Rightarrow A=B$$

$$e^{\frac{2\pi i k}{n}} = e^{\frac{2\pi i k'}{n'}},\quad 0\le k\le n-1,\quad n'\le n \Rightarrow n'=d$$

База: $\Phi_1(x) = x - 1$ — верно

Предположим, что верно для $j \leq k$ и докажем для $j = k+1$

$$\underbrace{\prod_{d \mid k+1} \Phi_d(x) = x^{k+1} - 1}_{\Downarrow}$$

$$\Phi_{k+1}(x) \cdot \prod_{\substack{d \mid k+1 \\ d \neq k+1}} \Phi_d(x)$$

$\in \mathbb{Z}[x]$

$\in \mathbb{Z}[x]$

коэф.-т при старшем члене равен 1

$$\Rightarrow \Phi_{k+1}(x) \in \mathbb{Z}[x] \qquad \triangleleft$$

Теорема Простых чисел вида $nk+1$ $(p \equiv 1 \pmod n)$ бесконечно много $\forall n \in \mathbb{N}$

Это слабый вариант (частный случай) теоремы Дирихле об арифм. прогрессиях:

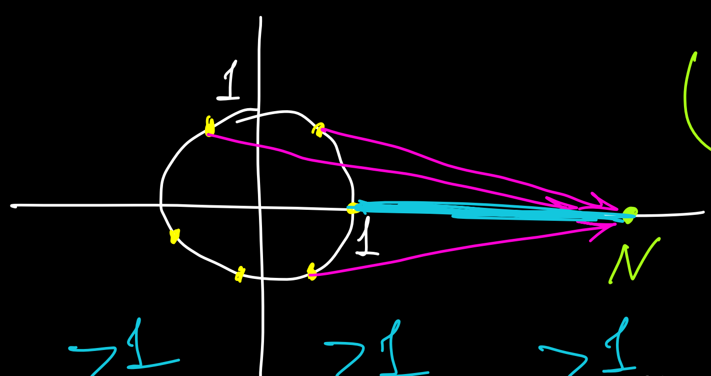
в $\forall$ арифм. прогр. с $(d, a_0)=1$ содерж. ∞ много простых чисел

$\triangleright$ Противное: $\exists\, p_1,\dots,p_k$ — полный список простых вида $ns+1$

Рассм. $N = np_1\dots p_k$

Рассм. $\Phi_n(N)$ и пусть $\underset{\text{простое}}{q} \mid \Phi_n(N)$

Заметим, что $\Phi_n(N) \neq \pm 1$.



$(N>2)$

$$|\Phi_n(N)| = \overset{>1}{|N-\xi|}\cdot\overset{>1}{|N-\xi^2|}\cdot\ldots\cdot\overset{>1}{|N-\xi^{\varphi(n)}|},$$ где

ξ — какой-то прим. корень n-й степени из 1

$\underset{>1}{|\Phi_n(N)|} = 1$ — невозможно

На самом деле, q не входит в этот список простых

$\Phi_n(N) \equiv \pm 1 \pmod N \Rightarrow (q, N) = 1$, т.е.

q — простое не из списка

$\Phi_n(0) = \pm 1$

$\sum_{(k,n)=1} k \,\vdots\, n$

$\prod_{d|n} \Phi_d(x) = \underbrace{x^n - 1}_{\vdots\, \Phi_n(x)}$

Предположим, что $N^m \equiv 1 \pmod q$, где

m — самое маленькое нат. число, обл. этим св.-ом

Заметим, что $N^n - 1 \,\vdots\, \underbrace{\Phi_n(N)}_{\vdots\, q} \Rightarrow$ $N^n \equiv 1 (q)$

$\Rightarrow N^n - 1 \,\vdots\, q \Rightarrow$ малая теор. Ферма $(q, N) = 1$

$N^{q-1} \equiv 1 (q)$

$\Rightarrow (q-1) \,\vdots\, n \Leftrightarrow q \equiv 1 (n)$

$$\left.\begin{aligned} N^n &\equiv 1 \pmod q \\ N^m &\equiv 1 \pmod q \end{aligned}\right\} \Rightarrow n = ms + l \Rightarrow$$

$$\Rightarrow N^n = N^{ms+l} =$$

$$= \underbrace{(N^m)^s}_{} \cdot N^l = 1 \cdot \boxed{N^l \equiv 1 \pmod q}$$

$l < m \Rightarrow \lightning \Rightarrow l = 0 \Rightarrow n \vdots m$

Итак, $n \vdots m$

Хотим: $\boxed{n = m}$

Пусть $m < n$ — предп. противное

Тогда $\prod_{d|m} \Phi_d(N) = N^m - 1 \equiv 0 \, (q)$

противоре

$\Rightarrow \Phi_{d_0}(N) \equiv 0 \, (\mathrm{mod}\ q)$

для некоторого $d_0 < n$

6

$2 \cdot 3 = 0$

$\Rightarrow N$ — корень кратности 2

у многочлена $\prod_{d|n} \Phi_d(x) = x^n - 1$

по mod q

$(x - N)$

$\Phi_{d_0}(N) \equiv 0 \, (\mathrm{mod}\ q)$ — см. выше

$\Phi_n(N) \equiv 0 \, (\mathrm{mod}\ q)$ — по опр.-ю q

$(x - N)$

$$\prod_{d|n} \Phi_d(x) \equiv \underbrace{(x-N)^2}(\text{что-то там})$$

А многочлен x^n-1 не имеет кратных корней по mod q.

Почему это так?

<u>Упр.</u> $P(x_0)=0$, P — мн.-н, x_0 — кратный корень

$P(x)=(x-x_0)^k Q(x)$, где $k \geq 2$

Тогда $P'(x_0)=0$, где $P'(x)$ — произв. мн.-на $P(x)$.

Но $(x^n-1)' = \cancel{n}x^{n-1} \equiv 0 \pmod q \Rightarrow x \equiv 0 \pmod q$

$(n,q)=1$, т.к. $\underset{n p_1 \ldots p_k}{N} \not\vdots\, q$

0 не явл. корнем $x^n-1 \Rightarrow$ у мн.-на x^n-1 нет кратных корней mod q. $\Rightarrow$

$\Longrightarrow m = n$