Простые числа и факториальность

1. Факториальность $\mathbb{Z}$ индукцией

   Любое натуральное число $n > 1$ единственным образом представляется в виде $n = p_1^{\gamma_1} \cdot \ldots \cdot p_\ell^{\gamma_\ell}$, где $p_1 < \ldots < p_\ell$ — простые числа.

   □ Пусть n — наименьшее натуральное число, которое можно представить в виде произведения простых двумя способами: $n = p_1 p_2 \ldots p_k$ и $n = q_1 q_2 \ldots q_m$. Рассмотрим число $(p_1 - q_1) p_2 \ldots p_k$, оно же $q_1(q_2 \ldots q_m - p_2 \ldots p_k)$. Его разложение должно быть единственным, но ни одно из чисел $p_1 - q_1$, p_2, …, p_k не может делиться на q_1. ■

2. Простые числа

   В евклидовых кольцах *простой* = *неприводимый*.

   p *простое*, если из $ab \,\vdots\, p$ следует, что $a \,\vdots\, p$ или $b \,\vdots\, p$.

   p *неприводимое*, если не существует таких необратимых x, y, что $p = xy$.

   Какие из $p \in \mathbb{P}$ остаются простыми в $\mathbb{Z}[\mathrm{i}]$?

   Ответ: $p \equiv_4 3$.

   □ Случай $p \equiv_4 3$. Пусть $p = (a + b\mathrm{i})(c + d\mathrm{i})$, то $|p|^2 = |a + b\mathrm{i}|^2 |c + d\mathrm{i}|^2 = (a^2 + b^2)(c^2 + d^2)$. Либо одно из чисел $a + b\mathrm{i}$, $c + d\mathrm{i}$ обратимо, либо $a^2 + b^2 = p = c^2 + d^2$. Но сумма двух квадратов не может давать остаток 3 при делении на 4.

   Случай $p \equiv_4 1$. По теореме Ферма-Эйлера, $p = x^2 + y^2$, а значит, $p = (x + y\mathrm{i})(x - y\mathrm{i})$. ■

3. Факториальность произвольного евклидового кольца

   Любой элемент факториального кольца единственным образом (с точностью до ассоциированности) раскладывается на простые множители.

   □ **Лемма.** Если $ac \,\vdots\, b$ и $(a, b) = 1$, то $c \,\vdots\, b$. Действительно, $1 = (a, b) = ak + bm$, отчего $c = ack + bcm \,\vdots\, b$.

   Значит, в любых двух разложениях на простые есть совпадающие, потому что если $r_1 r_2 \ldots r_k = q_1 q_2 \ldots q_m$, то $r_1 r_2 \ldots r_k \,\vdots\, q_1$, а значит, $r_1 \,\vdots\, q_1$ или $r_2 \ldots r_k \,\vdots\, q_1$, итд. ■

4. Факториально не значит евклидово

   Пример: $\mathbb{C}[t_1, t_2, \ldots, t_k]$.

5. p–показатели и лемма об уточнении степени

   $$\nu_p(n) = \max\{k : n \,\vdots\, p^k\}, \qquad \ln n = \sum_p \nu_p(n) \ln p, \qquad \nu_p(m!) = \sum_k \left\lfloor \frac{m}{p^k} \right\rfloor$$

$\nu_p(x^{mp}-1)=\nu_p(x^m-1)+1$ при условии, что $\nu_p(x^m-1)>1$ или $p>2$.

$\square$ Индукцией из разложения $x^{mp}-1=(x^m-1)(x^{m(p-1)}+x^{m(p-2)}+\ldots+x^m+1)$. $\blacksquare$

6. Постулат Бертрана

Для любого $n\in\mathbb{N}$ в множестве $\{n+1,\ldots,2n-1,2n\}$ есть простое число.

I $$\prod_{p\le x} p \le 4^{x-1}$$

II $\nu_p(C_{2n}^n)\le\log_p(2n)$, $\qquad p>\sqrt{2n}\Rightarrow\nu_p(C_{2n}^n)\le 1$, $\qquad \frac{2}{3}n<p\le n\Rightarrow\nu_p(C_{2n}^n)=0$

III $$\frac{4^n}{2n}\le C_{2n}^n\le\prod_{p\le\sqrt{2n}}2n\cdot\prod_{\sqrt{2n}<p\le\frac{2}{3}n}p\cdot\prod_{n<p\le 2n}p$$

IV если $\mathbb{P}\cap(n,2n]=\varnothing$, то $4^n\le(2n)^{1+\sqrt{2n}}\cdot 4^{\frac{2}{3}n}$, но это не так при $n>4000$

V числа 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001 простые.

Обобщение для больших чисел

$\forall\varepsilon>0\quad\exists n_0\quad\forall n>n_0\quad$ в промежутке $(n,n+\varepsilon n]$ есть простое число.

$\square$ Следует из закона распределения простых чисел. $\blacksquare$

7. * Теорема Чебышёва

$$\exists C_1,C_2>0\quad\forall n>n_0\quad C_1\frac{n}{\ln n}<\pi(n)<C_2\frac{n}{\ln n}.$$

$\square$

I $2^m\le C_{2m}^m<4^m$

II $m\ln 2\le\sum\limits_{p\le 2m}\ln p\le\pi(2m)\ln(2m)$

III $\boxed{\pi(n)>\frac{1}{6}\frac{n}{\ln n}}$

IV $m\ln 4\ge\sum\limits_{m<p\le 2m}\ln p\ge(\pi(2m)-\pi(m))\ln m$, т.е. $\pi(2m)-\pi(m)\le\ln 4\frac{m}{\ln m}$

V для $m=2^j\ge n^{19/20}$ получается $\pi(2^{j+1})-\pi(2^j)\le\ln 4\frac{2^j}{\frac{19}{20}\log_2 n}$

VI $\pi(n)-\pi(n^{19/20})<\frac{40\ln 4}{19}\frac{\frac{19}{20}\log_2 n+1}{\frac{19}{20}\log_2 n}\frac{n}{\ln(n)}$

VII $\boxed{\pi(n)<3\frac{n}{\ln n}}$ $\blacksquare$

Закон распределения простых чисел (Адамар и де ла Валле-Пуссен, 1896 г.)

$$\lim_{n\to\infty}\frac{\pi(n)}{n/\ln n}=1.$$