1 Uvod

Trditev 1.1. *Za vse $a, b \in \mathbb{R}$ ter vse $n \in \mathbb{N}$ velja*

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) = (a-b)\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right).$$

Če je n lih velja

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) = (a+b)\left(\sum_{i=0}^{n-1}(-1)^i a^i b^{n-1-i}\right).$$

Izrek 1.2 (Binomska formula). *Naj sta $a, b \in \mathbb{R}$ ter $n \in \mathbb{N}$. Velja*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

2 Pregled p-adične valuacije

Definicija 2.1. Naj bo $p \in \mathbb{P}$ ter $n \in \mathbb{N}$. *p-adična valuacija* števila n je tako nenegativno celo število $\nu_p(n)$, da velja

$$p^{\nu_p(n)} \mid n \quad \text{in} \quad p^{\nu_p(n)+1} \nmid n.$$

Lema 2.2. Osnovni izrek aritmetike *na alternativen način karakterizira p-adično valuacijo, namreč*

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Naslednje lastnosti so po alternativni karakterizaciji p-adičniosti očitne.

Izrek 2.3. *Za $x, y \in \mathbb{N}$ velja:*

- $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
- $\nu_p(x^y) = y \cdot \nu_p(x)$
- $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$. *Če velja $\nu_p(x) \neq \nu_p(y)$, potem sledi enakost.*

Trditev 2.4. *Naj so $a_1, a_2, \cdots, a_n$ naravna števila. Z oznakama* gcd *in* lcm *označujemo funkciji največji skupni delitelj in najmanjši skupni večkratnik. Velja:*

$$\gcd(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min\{\nu_p(a_1), \nu_p(a_2), \cdots, \nu_p(a_n)\}}$$

ter

$$\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\max\{\nu_p(a_1), \nu_p(a_2), \cdots, \nu_p(a_n)\}}.$$

Izrek 2.5 (Legendrova formula). *Naj bo $n \in \mathbb{N}$ ter $p \in \mathbb{P}$. Potem velja*

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Trditev 2.6. *Naj bo $n \in \mathbb{N}$ ter $p \in \mathbb{P}$. Potem velja*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1},$$

kjer $s_p(n)$ označuje vsoto števk števila n zapisanega v bazi p.

Trditev 2.7. *Za $n \in \mathbb{N}$ ter $p \in \mathbb{P}$ velja:*

$$n \cdot \frac{1 - \frac{1}{p^K}}{p-1} - \left\lfloor \log_p(n) \right\rfloor \leq \nu_p(n!) \leq \frac{n-1}{p-1},$$

oziroma rahlo poenostavljeno

$$\frac{n-p}{p-1} - \left\lfloor \log_p(n) \right\rfloor \leq \nu_p(n!) \leq \frac{n-1}{p-1} < \frac{n}{p-1}.$$

3 Dvig eksponenta

Lema 3.1. *Naj bo p liho praštevilo ter x, y tuji si celi števili.*

- *Če $p \mid x - y$ velja*
$$\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n).$$
- *Če $p \mid x + y$ in je n* ***lih*** *velja*
$$\nu_p(x^n + y^n) = \nu_p(x+y) + \nu_p(n).$$

Lema 3.2. *Naj bosta x, y lihi celi števili.*

- *Če $4 \mid x - y$ velja*
$$\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n).$$
- *Če $2 \mid x - y$ in n* ***sod*** *velja*
$$\nu_2(x^n - y^n) = \nu_2(x^2 - y^2) + \nu_2\left(\frac{n}{2}\right) = \nu_2(x+y) + \nu_2(x-y) + \nu_2(n) - 1.$$

Komentar 1. Velja zelo ohlapna ocena

$$\nu_p(n) \leq \log_p(n).$$