Proseminar B

Luka Horjak (luka.horjak@student.fmf.uni-lj.si)

12. marec 2021

Kazalo

Uvod

1 Modularna aritmetika

1.1 Praštevila

Definicija 1.1.1. $p \in \mathbb{N}$ je *praštevilo*, če je $p \neq 1$ in sta edina delitelja p enaka 1 in p.

Izrek 1.1.2 (Osnovni izrek aritmetike)**.** Vsako naravno število n lahko na enoličen način do vrstnega reda natančno zapišemo kot

$$n = \prod_{i=1}^{r} p_i^{k_i},$$

kjer so $p_i \in \mathbb{P}$ različna praštevila.

Dokaz. Induktivno lahko razcepimo vsako naravno število. Če ima neko število dva razcepa, lahko pokrajšamo vse skupne faktorje, nato pa nam na eni strani ostane neko praštevilo, ki ne deli druge strani, kar je seveda protislovje. □

Izrek 1.1.3. Množica $\mathbb{P}$ je neskončna.

Dokaz. Predpostavimo nasprotno. Potem

$$P = \prod_{p \in \mathbb{P}} p + 1$$

nima nobenega delitelja iz $\mathbb{P}$, kar je seveda protislovje. □

1.2 Teorija grup

Definicija 1.2.1. $(G, \circ)$ je *grupa*, če:

1. ima enoto: $\exists e \in G\ \forall a \in G \colon a \circ e = e \circ a = a$
2. vsak element ima inverz: $\forall a \in G\ \exists a^{-1} \in G \colon a \circ a^{-1} = a^{-1} \circ a = e$
3. $\circ$ je asociativna

Definicija 1.2.2. Za $a \in G$ rečemo, da je *končnega reda*, če $\exists m \in \mathbb{N} \colon a^m = e$. Najmanjšemu takemu m pravimo *red elementa*:

$$|a| = \min \{m \in \mathbb{N} \mid a^m = e\}.$$

Trditev 1.2.3. Če je $|a| = r \in \mathbb{N}$ in je $a^m = e$, $r \mid m$.

Dokaz. Če je $a^m = e$, je tudi $a^{m \bmod r} = e$, kar je protislovje, če $r \nmid m$. $\square$

Izrek 1.2.4 (Lagrange)**.** Naj bo H podgrupa končne grupe G. Potem

$$|H| \mid |G|.$$

Dokaz. Naj bo $A_x = \{xy \mid y \in H\}$. Očitno je A particija G na množice z močjo $|H|$. $\square$

Trditev 1.2.5. Če je G končna grupa, je vsak $a \in G$ končnega reda in velja

$$|a| \mid |G|.$$

Dokaz. Očitno obstajata $k < l$, da je $a^k = a^l$, saj je G končna. Potem je

$$e = a^k \circ a^{-k} = a^l \circ a^{-k} = a^{l-k}.$$

Naj bo $|a| = r$ in $A_a = \{e, a, \dots, a^{r-1}\}$. A je podgrupa G, zato smo končali po Lagrangu. $\square$

Trditev 1.2.6. Če je $(K, +, \cdot)$ kolobar z enico, je $K' = \{x \in K \mid \exists y \in K \colon xy = yx = 1\}$ grupa.

Dokaz. The proof is obvious and need not be mentioned. $\square$

1.3 Primes again

Izrek 1.3.1. Množica $\mathbb{P}$ je neskončna.

Dokaz. Naj bo $\hat{p} = 2^p - 1$ (Mersenovo število). Naj $q \mid \hat{p}$ za $p, q \in \mathbb{P}$. Potem je p red 2 po modulu q, zato $p \mid q - 1$, torej je $q > p$. □

Trditev 1.3.2. Različni Fermatovi števili $F_n = 2^{2^n}$ sta si tuji.

Dokaz. Velja

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

□

1.4 Porazdelitev praštevil

Za $x \in \mathbb{R}$ definiramo
$$\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|.$$

Definirajmo $\log x = \displaystyle\int_1^x \frac{1}{t}\, dt$. Sledi, da je

$$\log x \leq \sum_{i=1}^{\lfloor x \rfloor} \frac{1}{i} \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq n}} \frac{p}{p-1} \leq \pi(x) + 1,$$

saj je $p_i \geq i + 1$.

Izkaže se, da tudi $\displaystyle\sum_{p \in \mathbb{P}} \frac{1}{p}$ divergira.

Definicija 1.4.1. Prašteviloma p in $p+2$ pravimo *praštevilska dvojčka.*

Izrek 1.4.2 (Wilson)**.** Naravno število $p > 1$ je praštevilo natanko tedaj, ko je

$$(p-1)! + 1 \equiv 0 \pmod p.$$

Dokaz. Če je p praštevilo, lahko vsa manjša števila razen 1 in $p-1$ združimo v inverzne pare, saj iz $x^2 \equiv 1 \pmod p$ sledi $x \equiv \pm 1 \pmod p$. Sledi, da je

$$(p-1)! + 1 \equiv 1 \cdot 1^{\frac{p-3}{2}} \cdot -1 + 1 \equiv 0 \pmod p.$$

V nasprotnem primeru lahko p zapišemo kot $a \cdot b$, kjer je $1 < a < b < p$ z izjemo, ko je p kvadrat praštevila. Sledi
$$(p-1)! + 1 \equiv 1 \pmod a,$$
zato $a \nmid (p-1)! + 1$. $\square$

Izrek 1.4.3. Števili m in $m+2$ sta praštevilska dvojčka natanko tedaj, ko je

$$4((m-1)! + 1) + m \equiv 0 \pmod{m(m+2)}.$$

1.5 Porazdelitev praštevil

Izrek 1.5.1. Velja
$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

Definicija 1.5.2. Naj bosta $f, g\colon [0, \infty) \to \mathbb{R}$. Oznaka
$$f = \Theta(g)$$
pomeni, da obstajata taki konstanti $c, d > 0$, da je
$$cg(x) \leq f(x) \leq dg(x)$$
za velike x.

Oznaka
$$f = \Omega(g)$$
pomeni, da obstaja taka konstanta $c > 0$, da je
$$cg(x) \leq f(x)$$
za velike x.

Izrek 1.5.3 (Čebišev)**.** Velja
$$\pi(x) = \Theta\left(\frac{x}{\log x}\right)$$

Lema 1.5.4. Velja
$$\binom{2m}{m} \geq \frac{2^{2m}}{2m} \quad \text{in} \quad \binom{2m+1}{m} < 2^{2m}.$$

Definicija 1.5.5. Za $n \in \mathbb{N}$ in $p \in \mathbb{P}$ označimo
$$\nu_p(n) = \max\left\{k \mid p^k \mid n\right\}.$$

Lema 1.5.6. Velja
$$\nu_p(n!) = \sum_{k\in\mathbb{N}} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Dokaz. The proof is obvious and need not be mentioned. □

Izrek 1.5.7. Za vsa naravna števila $n \geq 2$ velja
$$\pi(n) \geq \left(\frac{\log 2}{2}\right) \frac{n}{\log n}.$$

Dokaz. Velja

$$\nu_p \binom{2m}{m} = \nu_p((2m)!) - 2\nu_p(m!) = \sum_{k \geq 1} \left(\left\lfloor \frac{2m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor \right).$$

Seveda pa je

$$\sum_{k \geq 1} \left(\left\lfloor \frac{2m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor \right) \leq \frac{\log(2m)}{\log p},$$

saj so vsi členi največ 1, za $k > \frac{\log(2m)}{\log p}$ pa so vsi enaki 0. Velja pa

$$\begin{aligned}
\pi(2m)\log(2m) &= \sum_{p \leq 2m} \frac{\log(2m)}{\log p} \cdot \log p \\
&\geq \sum_{p \leq 2m} \nu_p \binom{2m}{m} \log p \\
&= \log \binom{2m}{m} \\
&\geq \log \left(\frac{2^{2m}}{2m} \right) \\
&\geq m \log 2.
\end{aligned}$$

Sledi

$$\pi(2m) \geq \frac{m \log 2}{\log 2m} = \frac{\log 2}{2} \cdot \frac{2m}{\log 2m}.$$

Ker je $\pi(2m) = \pi(2m-1)$ in je $\frac{x}{\log x}$ naraščajoča, smo končali. □

Posledica 1.5.7.1. Velja

$$\pi(x) = \Omega\left(\frac{x}{\log x} \right).$$

Dokaz. Velja

$$\pi(x) = \pi(n) \geq \left(\frac{\log 2}{2} \right) \frac{n}{\log n} \geq \left(\frac{\log 2}{2} \right) \frac{x}{\log x} - \frac{\log 2}{2 \log x},$$

zato vzamemo $c = \frac{\log 2}{2} - \varepsilon$. □