Алгебарске структуре - Ојлерова функција

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Група

Нека је дат непразан скуп S, на ком је дефинисана бинарна операција

$$+ : S \times S \to S.$$

1. Уређени пар $(S, +)$ се назива **групоид**.
2. Групоид, у ком је операција **асоцијативна** $+$ се назива **полугрупа**.
3. Полугрупа са **јединичним елементом** се назива **моноид**.
4. Моноид у ком сваки елемент има **инверз** је **група**.
5. Ako је операција $+$ комутативна, онда је $(S, +)$ **Абелова група**.

Прстен

Нека је дат скуп S, на ком су дефинисане двије бинарне операције

$$+ : S \times S \to S,$$

$$\bullet : S \times S \to S.$$

Уређена тројка $(S, +, \bullet)$ је прстен ако

1. $(S, +)$ је Абелова група.
2. $(S, \bullet)$ је полугрупа.
3. За свако $a, b, c \in S$ вриједи дистрибутивност множења у односу на сабирање

$$a \bullet (b + c) = a \bullet b + a \bullet c,$$

$$(a + b) \bullet c = a \bullet c + b \bullet c.$$

Поље

Нека је $(S, +, \bullet)$ прстен. Дефинишимо

$$S' = S \setminus \{0\}.$$

Ако је $(S', \bullet)$ Абелова група, онда $(S, +, \bullet)$ називамо **пољем**.

Примјер

Нека је $\mathbb{Z}_p$ скуп остатака по модулу p. Тада је $(\mathbb{Z}_p, +, \cdot)$ поље, гдје су сабирање и множење по модулу p.

Често, умјесто $\mathbb{Z}_p$ користимо ознаку $\mathbb{F}_p$.

Мултипликативни инверз по модулу

Већ смо нагласили да је један од важнијих појмова у модуларној аритметици појам **мултипликативног инверза**.

Лема

Нека су a и m природни бројеви. Тада је

$$a \cdot b \equiv 1 \pmod{m} \text{ за неко } b \in \mathbb{N} \text{ акко } \textbf{нзд}(a, m) = 1.$$

Број b називамо мултипликативним инверзом броја a по модулу m.

$$[\textbf{нзд}(a, m) = 1 \leftrightarrow ax + my = 1.]$$

Напримјер, бројеви $1, 3, 5, 9, 11, 13$ имају мултипликативне инверзе по модулу 14.

Ојлерова ϕ функција

Основна структура модуларне аритметике по модулу m је **прстен** цијелих бројева

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}.$$

Унутар овог скупа, налази се, као што смо нагласили група јединица по модулу m, односно мултипликативних инверза $(\mathbb{Z}/m\mathbb{Z})^*$,

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} \mid \textbf{нзд}(a, m) = 1\}.$$

Једна од најпознатијих и вјероватно најважнијих функција у класичној аритметици је Ојлерова ϕ функција, коју дефинишемо једноставно као

$$\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|.$$

Мултипликативност Ојлерове ϕ функције

Подсјећајући се дефиниције Ојлерове функције, лако се изводи закључак да је

$$\phi(p) = p - 1, \text{ односно } \phi(p^k) = p^k - p^{k-1},\ k \in \mathbb{N},$$

гдје је p прост број. Међутим, наш циљ је да нађемо формулу за Ојлерову функцију за сваки природан број и у том смислу ће нам од помоћи бити следећа теорема.

Теорема

Ојлерова функција је мултипликативна. То значи да за природне бројеве m, n такве да **нзд**$(m, n) = 1$, вриједи

$$\phi(mn) = \phi(m)\phi(n).$$

Формула за Ојлерову функцију

Директна последица претходне теореме је следећи закључак.

Последица

Нека је $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ факторизација природног броја n. Тада је

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Напримјер,

$$\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = 60 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16.$$

Ред елемента у групи

Нека је дата група $(G, \bullet)$, са јединичним елементом , и произвољан елемент $a \in G$. Претпоставимо да постоји природан број n такав да $a^n = e$.

Најмањи такав број $n \in \mathbb{N}$ је **ред елемента** a у групи G.

Ако је група коначна, тада број елемената у њој називамо **редом групе**.

Лема - посљедица Лагранжове теореме

Нека је дата коначна група $(G, \bullet)$. Тада је ред сваког елемента у њој коначан и дијели ред групе.

Ојлерова теорема

Стигли смо до важне теореме која се веома често користи, како у теоријским разматрањима, тако и у неким практичним проблемима. Ова теорема има значајно мјесто у разумијевању неких важних крипто-алгоритама међу којима је најпознатији RSA.

Ојлерова теорема

Ако је **нзд**$(a, m) = 1$, за природне бројеве a, m, онда је

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Фермаова теорема

Последица Ојлерове теореме, односно њен специјалан случај је чувена Фермаова теорема.

Фермаова теорема

Ако је p прост број и p не дијели a, онда је

$$a^{p-1} \equiv 1 \pmod{p}.$$

Последично, ако је p прост број и a произвољан цио број, тада важи $a^p \equiv a \pmod{p}$.

Примјер

За произвољно $\epsilon > 0$ постоји природан број n тако да

$$\frac{\phi(n)}{n} > 1 - \epsilon.$$

Пошто је скуп простих бројева бесконачан, онда за свако $\epsilon > 0$ постоји прост број p тако да $p > 1/\epsilon$. За $n = p$, имамо да

$$\frac{\phi(n)}{n} = 1 - \frac{1}{p} > 1 - \epsilon.$$

Теорема

(Вилсон) Ако је p прост број, онда је

$$(p-1)! \equiv -1 \pmod{p}.$$

За $p = 2$ или $p = 3$, тврдња је очигледно тачна. Нека је p прост број већи од 3, а скуп

$$S = \{2, 3, \ldots, p-2\}.$$

Ако посматрамо конгруенције $ax \equiv 1 \pmod{p}$, за $a \in S$, јасно је да постоји рјешење, да је јединствено и да се налази у скупу S. Такође, рјешење претходне конгруенције је различито од a јер би у супротном било

$$a^2 \equiv 1 \pmod{p}, \text{ односно } p|(a-1)(a+1),$$

а што није могуће јер $a \leq p-2$. Зато се елементи S међусобно "неутралишу".

Питања и задаци

Користећи наведене теореме, можемо лако рјешавати одређене врсте проблема

Питање

Како једноставно израчунати инверз од 7814 модуло 17449, ако је дато да је 17449 прост број?

Задатак

Наћи остатак при дијељењу 2^{154} са 13.

Генератор мултипликативне групе коначног поља

Фермаова теорема дефинише једну важну особину јединица (елемената различитих од нуле) у коначном пољу. Овдје помињемо једну веома важну особину коначног поља које има једнако теоретску и практичну вриједност.

Теорема о примитивном коријену

Нека је p прост број.Тада постоји елемент $g \in \mathbb{F}_p^*$ који генерише сваки елемент из $\mathbb{F}_p^*$, односно

$$\mathbb{F}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}.$$

Елементи који имају особину се зови примитивним коријенима или **генераторима** $\mathbb{F}_p^*$.

Хвала на пажњи :)