

عنوان

نام نویسنده

دانشگاه پیام نور تهران

## ۱ قضیه باقیمانده چینی

قضیه باقیمانده چینی دو کاربرد مهم دارد. فرض کنید عدد صحیح  $n$  به صورت  $n = n_1 \cdot n_2 \dots n_k$  تجزیه شود که عوامل  $n_i$  دو به دو نسبت به هم اول هستند. اولاً، قضیه باقیمانده چینی، یک ساختاری توصیفی است که ساختار  $Z_n$  را مثل ضرب دکارتی  $Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_k}$  توصیف می کند، به طوری که در مولفه  $i$  ام، ضرب و جمع مولفه ای به پیمانه  $n_i$  انجام می شود. ثانیاً، این توصیف می تواند منجر به الگوریتم های کارآمدی شود، زیرا کارکردن در هر سیستم  $Z_{n_i}$  می تواند (بر حسب عملیات بیتی) کارآمدتر از کارکردن به پیمانه  $n$  باشد.