دانشکده مهندسی کامپیوتر

استاد درس: دکتر ابوالفضل دیانت

بهار ۱۴۰۳

تمرین زنون

امنیت سیستم های کامپیوتری

گزارش تمرین

ستاره باباجانی - ملیکا محمدی فخار

۹۹۵۲۲۰۸۶-۹۹۵۲۱۱۰۹

۱ سوال اول

۱.۱ Eratosthenes of Sieve

سریع‌ترین الگوریتمی که میان الگوریتم‌های متعدد تجزیه اعداد اول وجود دارد، الگوریتم "سوئیب اراتوستن" است.

سوئیب اراتوستن یک الگوریتم تخته چوبی برای یافتن اعداد اول در بازه اعداد مشخص است. مراحل اجرای الگوریتم به شرح زیر است:

۱. یک جدول از اعداد ۱ تا n ایجاد می‌شود.
۲. شماره‌های اولیه (۱ و ۲) به عنوان اعداد اول در نظر گرفته می‌شوند.
۳. از اولین عدد اول (۲) شروع به حذف تمامی ضرب‌های آن در بازه اعداد می‌شود.
۴. ادامه این فرآیند بر روی اعداد باقی‌مانده تا جایی که نیاز باشد.
۵. اعداد باقی‌مانده در نهایت، اعداد اول هستند.

سوئیب اراتوستن با پیچیدگی زمانی O(n log log n) یکی از سریع‌ترین الگوریتم‌ها برای تجزیه اعداد اول است. البته، وجود الگوریتم‌های دیگر نیز بستگی به نوع و ساختار مسئله دارد.

۲.۱ Sieve Field Number General

غربال میدان اعداد عمومی (GNFS) سریع ترین الگوریتم شناخته شده برای فاکتورگیری اعداد بزرگ است و به ویژه در زمینه رمزنگاری کاربرد دارد. این الگوریتم عمدتاً برای فاکتورسازی اعداد صحیح به جای تجزیه اول استفاده میشود. پیچیدگی زمانی GNFS زیر نمایی است، به طور خاص اعتقاد بر این است که در محدوده L(۱/۳) است، که در آن L نماد L-notation است که پیچیدگی زمانی زیر نمایی sub exponential را نشان می دهد. به عبارت ساده تر، سریعتر از زمان نمایی است اما همچنان سریعتر از زمان چند جمله ای رشد می کند. به دلیل ماهیت الگوریتم‌های نمایی فرعی، بیان پیچیدگی دقیق از نظر نمادهای آشنای big-O دشوار است.

۲ سوال دوم

اعداد Semiprime یا نیمه اول اعدادی طبیعی هستند که دقیقاً دو عدد اول به عنوان عوامل آنها وجود دارد. به عبارت دیگر، یک عدد semiprime به صورت p * q قابل نمایش است، جایی که p و q اعداد اول هستند.

برای مثال، اگر p = ۵ و q = ۳ باشند، آنگاه $15 = 3 \times 5$ یک عدد semiprime خواهد بود. و یا اگر p = ۱۱ و q = ۷ باشند، آنگاه $77 = 7 \times 11$ نیز یک عدد semiprime است.

تجزیه اعداد نیمه اول می تواند آسان تر از تجزیه اعداد ترکیبی باشد، به خصوص زمانی که با اعدادی مقایسه می شود که تعداد زیادی عامل اول دارند. این به این دلیل است که نیمه اول ها فقط دو عامل اول دارند که فرآیند فاکتورسازی را ساده تر می کند.

امنیت برخی از الگوریتم‌های رمزنگاری مانند RSA، بر دشواری فاکتورگیری حاصل ضرب دو عدد اول

بزرگ متکی است. Semiprime اغلب به عنوان مبنایی برای این الگوریتم‌ها انتخاب می‌شوند، زیرا اعتقاد بر این است که فاکتورسازی آنها یک مشکل محاسباتی دشوار است. با این حال، با ظهور منابع محاسباتی قدرتمند و الگوریتم‌های فاکتورسازی پیشرفته‌تر، امنیت برخی از Semiprime های کوچک‌تر مورد استفاده در سیستم‌های رمزنگاری قدیمی‌تر، آسیب‌پذیر شده است.

به طور خلاصه، تجزیه اعداد Semiprime می تواند آسان تر از تجزیه اعداد مرکب دیگر باشد، اما دشواری آن همچنان به اندازه اعداد اول درگیر و الگوریتم های فاکتورگیری به کار گرفته شده بستگی دارد.