تمرین اسلاید 30 فصل سوم

عرفان زارع

امیررضا ویشته

زمستان 1402

Question:

✍ پیچیدگی زمانی سریع‌ترین الگوریتم برای تجزیه اعداد اول چگونه است؟

✍ اعداد Semiprime چیست؟ تجزیه این اعداد نسبت به سایر اعداد پیچیده‌تر است یا ساده‌تر؟

(1

در هنگام جست و جو به سه الگوریتم سریع متفاوت برای یافتن تجزیه اعداد ، رسیدیم . حال مقایسه ای میان آنها انجام داده و نتیجه و جواب نهایی براساس این مقایسه داده می شود.

الگوریتم SNFS(Special Number ،GNFS(Gneral Number Field Sieve Field Sieve) و ECM :

الگوریتم ECM دارای پیچیدگی زمانی از اردر

$O(\exp(C(\log n)^{1/2}(\log\log n)^{2/3}))$ در حالت میانگین می باشد. برای اعداد با اندازه متوسط، ECM می تواند در مقایسه با روش های دیگر کارآمد و سریعتر باشد. ولی، برای اعداد بسیار بزرگ، ECM ممکن است با الگوریتم های پیشرفته تر مانند GNFS و SNFS بهتر عمل کند و خود ECM نتیجه خوبی ندارد.

الگوریتم GNFS,SNFS هردو دارای اردر زمانی

$O(\exp((C(\log n)^{1/3}(\log\log n)^{2/3}))$ هستند و این دو الگوریتم ، قدرتمند ترین الگوریتم های شناخته شده برای تجزیه اعداد اول می باشند و به شدت سریعتر از الگوریتم ECM برای اعداد بزرگ هستند که انهارا به روش های انتخابی برای اعداد با اهمیت رمزنگاری تبدیل می کند.

2)

اعداد نیمه اول ، اعداد مرکبی اند که تنها از ضرب دو عدد اول حاصل شده اند و این دو عدد مجزا از یکدیگر اند. تجزیه اعداد نیمه اول به ضرایب اول آنها معمولا پیچیده تر از اعداد کوچکتر یا خود اعداد اول است. این بدان دلیل است که نیمه نخست‌ها عمدتاً برای استفاده در رمزنگاری انتخاب می‌شوند، جایی که فاکتورسازی آنها به اعداد اول عمدتاً برای اطمینان از امنیت سیستم‌های رمزنگاری چالش برانگیز و دشوار است.

برای اعداد نیمه اول کوچک، تجزیه ممکن است با استفاده از الگوریتم هایی مانند تقسیم آزمایشی، الگوریتم Pollard's Rho یا حتی ECM نسبتاً ساده باشد، ولی با افزایش اندازه اعداد نیمه اول، فاکتورسازی به طور قابل توجهی چالش برانگیز و سخت تر می شود. برای اعداد نیمه اول بزرگتر مورد استفاده در سیستم های رمزنگاری جدید (که حاصل ضرب دو عدد اول بسیار بزرگ هستند)، الگوریتم های تخصصی مانند غربال میدان عددی عمومی (GNFS) یا غربال میدان عددی ویژه (SNFS) استفاده می شود. این الگوریتم‌ها بسیار بهینه‌سازی و طراحی شده‌اند تا پیچیدگی فاکتورگیری اعداد نیمه‌اول بزرگ را به طور کارآمد مدیریت نمایند.

مشکل در تجزیه اعداد نیمه اول، از عوامل مهم کاربرد آنها در رمزنگاری است. به ویژه در رمزگذاری نامتقارن که در آن امنیت سیستم به ناتوانی در تجزیه سریع اعداد نیمه اول بزرگ به اجزای اول آنها وابسته است.