پردیس علوم
دانشکده ریاضی، آمار و علوم کامپیوتر

غربال میدان عددی و روش‌های مدرن تجزیه

نگارنده

خشایار باروتی

استاد راهنما: دکتر امیر قادر مرزی

پایان نامه برای دریافت درجه کارشناسی
در رشته علوم کامپیوتر

تابستان ۹۶

چکیده

غربال در لغت به معنی الک کردن است. این مفهوم در تجزیه‌اعداد اولین بار توسط اراتستن برای پیدا کردن اعداد اول استفاده شد. ایده‌ی این الگوریتم ، که دلیل نام‌گذاری آن نیز می باشد، در الگوریتم‌های مدرن تجزیه نیز مورد استفاده قرار گرفت. یک نمونه از این الگوریتم‌ها غربال میدان عددی است.

در این گزارش به بررسی این روش ، بررسی مشکلات موجود در پیاده‌سازی این الگوریتم می‌پردازیم و در بخش آخر یک نمونه از کاربردهای این الگوریتم در تجزیه‌ی عدد ۱۵۵ رقمی F_9 ،عدد ۹ام فرما را مورد بررسی قرار می‌دهیم.

پیشگفتار

نظریه ی اعداد یکی از قدیمی‌ترین و مورد توجه‌ترین شاخه‌های ریاضی می‌باشد که طی سال ها پیشرفت‌های زیادی در آن انجام گرفته و ارتباط زیادی با دیگر شاخه‌های ریاضی پیدا کرده است.
با پیدایش علوم کامپیوتر انشعابات جدیدی در نظریه ی اعداد به وجود آمدند و مسائل الگوریتمیک در نظریه ی اعداد که از قبل مطرح بودند، اهمیت بیشتری یافتند.
دوتا از معروف ترین این مسائل، محک اول بودن یک عدد، و تجزیه ی یک عدد به عوامل اول آن‌اند.
این دو مسئله، دو مسئله ی بسیار دشوار در نظریه ی محاسباتی اعدادند و پیدا کردن یک الگوریتم از مرتبه ی زمانی چندجمله‌ای برای حل این مسائل، از مسائل دشوار نظریه اعداد و نظریه الگوریتم می باشد.
دشواری این مسائل باعث شد که تجزیه ی اعداد پایه‌ی مناسبی برای روش‌های رمزنگاری کلید عمومی باشد و برای مثال روش‌هایی مانند RSA به وجود آمدند که امنیت و قدرت آن‌ها به دلیل دشواری مسئله ی تجزیه می‌باشد.
رایج شدن RSA موجب توجه بیشتر به مسئله ی تجزیه شد و الگوریتم های زیادی با استفاده از ابزارهای مختلف ریاضیات برای حل این مسئله معرفی شدند.

غربال میدان های عددی، یکی از این الگوریتم ها برای حل مسئله ی تجزیه است که در دهه ی ۹۰ میلادی توسط لنسترا معرفی شد. این الگوریتم از ابزارهای نظریه ی جبری اعداد برای حل این مسئله استفاده می کند.
این الگوریتم متنی بر نوشتن عدد ورودی الگوریتم تجزیه یا مضربی از آن به شکل تفاضل دو مربع کامل است که اولین بار توسط اویلر مورد استفاده قرار گرفت. دشواری این روش به پیدا کردن این دو مربع کامل است. برای حل این مشکل از الگوریتم غرباب استفاده خواهیم کرد. با استفاده از غربال می‌توان تعدادی عدد اول انتخاب کرد (معمولا اعداد کمتر از یک کران مناسب) و اعداد یک بازه‌ی داده شده را که همه‌ی عوامل اولشان در مجموعه‌ی از پیش تعیین شده باشد، تجزیه می‌کنیم. حال اگر تعداد مناسبی عدد تجزیه شده داشته باشیم ، می توانیم تعدادی از آن ها را بیابیم که ضربشان مربع کامل باشد.

به طور دقیق‌تر ما به دنبال $X \cong Y \mod N$ هستیم که X, Y در یک پایه‌ی تجزیه‌ی به نسبت کوچک قابل تجزیه باشند و با ضرب دو طرف اینگونه معادلات در هم تلاش می‌کنیم دو طرف هم‌نهشتی مربع کامل شوند.

در غربال میدان عددی از همین ایده استفاده می‌شود ولی در این الگوریتم از یک هم‌ریختی حلقه‌ای از حلقه‌ی اعداد صحیح جبری یک میدان عددی به $\mathbb{Z}_N$ استفاده می‌شود و این بار به دنبال یک مربع کامل در این حلقه می‌گردیم که تصویر آن نیز یک مربع کامل باشد سپس با استفاده از این همریختی یک جواب برای $X^2 \cong Y^2 \mod N$ می‌یابیم.

در این گزارش به بررسی الگوریتم غربال میدان عددی ، بررسی مشکلات این الگوریتم و روش‌های پیشنهادی برای رفع این مشکلات می‌پردازیم.

فهرست مطالب

فصل ۱

مفاهیم مقدماتی

در این بخش به تعاریف و قضایا ی مورد نیاز برای مطالعه ی مطالب بخش های بعد خواهیم پرداخت.

۱.۱ نظریه جبری اعداد :

تعریف: $a \in \mathbb{C}$ را جبری نامیم هرگاه ریشه ی یک چندجمله ای $p \in \mathbb{Q}[x]$ باشد.

تعریف: $a \in \mathbb{C}$ را عدد صحیح جبری گوییم هرگاه برای یک چند جمله ای تکین با ضرایب صحیح ، a ریشه ی آن باشد.

تعریف: گسترش K از $\mathbb{Q}$ را یک میدان عددی گوییم هرگاه $[K : \mathbb{Q}] < \infty$.

قضیه: توسیع $\mathbb{Q}(\alpha)$ یک میدان عددی است اگر و فقط اگر α جبری باشد.

قضیه: مجموعه ی همه ی اعداد جبری در $\mathbb{Q}$ تشکیل یک میدان می دهد.
مجموعه ی همه ی اعداد صحیح جبری یک میدان عددی یک زیر حلقه از آن است و آن را با Z_K نایش می دهیم.

قضیه: اگر K یک میدان عددی باشد و Z_K حلقه ی اعداد صحیح آن باشد، می توان اعداد صحیح جبری $\alpha_1, ..., \alpha_k$ را چنان یافت که $Z_K = \mathbb{Z}[\alpha_1, ..., \alpha_n].\alpha_1, ..., \alpha_n$ را پایه‌ی صحیح برای Z_k می‌نامیم.

تعریف: اگر $\alpha \in K$ ، نرم این عضو را ضرب تصاویر آن تحت نشاندن های مختلف $K \to \mathbb{C}$ تعریف می کنیم.

نکته: بسیاری از میدان های عددی حوزه‌ی تجزیه یکتا نیستند.

یکی از مشکلات اصلی در حل مسایل درمیدان‌های عددی عدم وجود تجزیه‌ی یکتا است. که برای رفع این مشکل از ایده‌آل‌های Z_K استفاده می‌کنیم.

تعریف: اگر I یک ایده آل Z_K باشد ، تعریف می کنیم $N(I) = |Z_K/I|$ (نرم ایده آل)

قضیه: اگر $\alpha \in Z_K$ ، داریم که $N(< \alpha >) = N(\alpha)$

نکته: طبق قضیه قبل نرم یک ایده آل اصلی همواره عضو آن است.

نکته: نرم یک ایده آل اول همواره توان یک عدد اول است ، زیرا در میدان های عددی ایده آل های اول ماکسیمال اند و در نتیجه Z_K/p یک میدان متناهی می شود.
به علاوه نرم عضو این ایده آل است و چون ایده آل اول است اگر $N(q) = p^k$ ، داریم که $p \in q$.

قضیه: هرچند در Z_K لزوما یکتایی تجزیه وجود ندارد ولی هر ایده آل Z_K به طور یکتا به ایده آل های اول تجزیه می شود.

تعریف: یک ایده آل کسری Z_K یک زیر مجموعه ی K به شکل $(1/\lambda)C$ است که C یک ایده آل Z_K است و $\lambda \in Z_K$.

تعریف: اگر $\mathfrak{B}_K$ گروه همه ی ایده آل های کسری Z_K و $\mathfrak{BF}_K$ گروه همه ی ایده آل های کسری اصلی Z_K باشد ، گروه رده ای $C_K = \mathfrak{B}_K/\mathfrak{BF}_K$ می باشد و اندازه‌ی آن را عدد رده ای می نامیم.

قضیه: عدد رده ای همواره متناهی است.

قضیه(ددکیند_ کومر): فرض کنید $K = \mathbb{Q}[\theta]$ و چند جملهای مینیمال θ ، $T(X)$ باشد. $f = [Z_k : \mathbb{Z}[\theta]]$. برای هر $p \in \mathbb{P}$ که f را عاد نکند اگر داشته باشیم :

$$T(X) \cong \prod_{i=1}^{g} T_i(X)^{e_i} \mod p$$

تجزیه ی $T(X)$ به عوامل تحویل ناپذیر در $\mathbb{F}_p[X]$ باشد و T_i ها تکین باشند ، خواهیم داشت

$$pZ_k = \prod_{i=1}^{g} {p_i}^{e_i} \text{ ، } p_i = (p, T_i(\theta))$$

و p_i ها ایده آل های اولند.

۲.۱ پیچیدگی محاسباتی و مرتبه ی زمانی:

نظریهٔ پیچیدگی محاسباتی) شاخه‌ای از نظریهٔ محاسبات، علوم نظری رایانه و ریاضی است که به بررسی دشواری حل مسائل به وسیلهٔ رایانه (به عبارت دقیق‌تر به صورت الگوریتمی) می‌پردازد. این نظریه بخشی از نظریهٔ محاسباتی است که با منابع مورد نیاز برای حل یک مسئله سروکار دارد.

عمومی‌ترین منابع، زمان (مقدار زمان مورد نیاز برای حل مسئله) و فضا (مقدار حافظه مورد نیاز) می‌باشند. دو مفهوم اصلی این بخش ، مفهوم O بزرگ و مفهوم P و NP می باشند.

تعریف: اگر f،g توابعی روی یک زیر مجموعه از $\mathbb{R}$ باشند ، می گوییم $f = O(g)$ اگر و تنها اگر اعداد حقیقی M ، x_0 چنان موجود باشند که ، $f(x) < Mg(x)$ برای هر $x > x_0$.

مثلا $x = O(x^2)$ ولی $x \neq O(\log(x))$.

معروف‌ترین کلاس‌های پیچیدگی، P و NP هستند که مسئله‌ها را از نظر زمان مورد نیاز تقسیم‌بندی می‌کنند. به طور شهودی می‌توان گفت P کلاس مسئله‌هایی است که الگوریتم‌های سریع برای پیدا کردن جواب آن‌ها وجود دارد. اما NP شامل آن دسته از مسئله‌هاست که اگرچه ممکن است پیدا کردن جواب برای آن‌ها نیاز به زمان زیادی داشته باشد اما چک کردن درستی جواب به وسیلهٔ یک الگوریتم سریع ممکن است. البته کلاس‌های پیچیدگی به مراتب سخت‌تری از NP نیز وجود دارند.

۳.۱ رمز نگاری کلید عمومی :RSA

RSA يكي از اولين روش های رمزنگاری با کلید عمومی است. در این سبک از رمزنگاری ها یک کلید به عنوان کلید عمومی برای رمز گذاری به اشتراک گذاشته می شود و کلید دیگری برای رمزگشایی به طور خصوصی انتخاب می شود.

RSA در سال ۱۹۷۸م. توسط ریوست [۱] و شمیر [۲] و آلدمان [۳] به وجود آمد. RSA از ۴ مرحله ی اصلی ساخت کلید ، اشتراک گذاری کلید ، رمزگذاری و رمزگشایی تشکیل شده است.که به ترتیب به شرح زیرند .

ساخت کلید: دو عدد اول p و q را در نظر بگیرید. (بسیار بزرگ)
e را طوری انتخاب می کنیم که $(e, \phi(pq)) = 1$ و d را اینگونه انتخاب می کنیم که $e^{-1} \cong d \mod \phi(pq)$

حال (pq, e)کلید عمومی و d کلید خصوصی است.

توزیع کلید: فرض کنید A می خواهد یک پیغام برای B بفرستد. ،A پیام خود را با کلید عمومی B رمزگذاری می کند و B با کلید خصوصی خود، پیام A را رمزگشایی می کند.

رمزگذاری: فرض کنید A می خواهد پیام M را به B با کلید عمومی (pq, e) بفرستد. برای این کار A $C = M^e(\mod pq)$ را محاسبه می کند و متن رمزشده ی C را برای B می فرستد.

رمزگشایی: B که متن رمزشده ی C را از A دریافت کرده، کلید عمومی $C = M^e$ پس داریم که$M \cong C^d \cong (M^e)^d(\mod pq)$ که پیام A است.

برای محاسبه d از روی (pq, e) نیازمند به پیدا کردن$\phi(pq)$ هستیم. که این امر نیازمند تجزیه ی $n = pq$ است و اگر p و q اعداد اول بزرگ باشند این امر کار بسیار دشواری است.

رایج شدن RSA به اهمیت مسئله ی تجزیه و پیدا کردن اعداد اول بزرگ افزود.

---

[۱] Rivest R.
[۲] Shamir A.
[۳] Aldeman L.

فصل ۲

غربال مربعی

غربال مربعی[۱] یک روش تجزیه ی سریع است که در دهه ی ۸۰ میلادی توسط پومرانس معرفی شد.

ایده ی اصلی این روش پیدا کردن دو مربع کامل همنهشت به پیمانه ی عدد ورودی الگوریتم تجزیه است. یعنی برای تجزیه ی N تلاش می کنیم x ، y را چنان می یابیم که $x^2 \cong y^2 \mod N$. که نتیجه می دهد $N|(x-y)(x+y)$ و اگر x ، y کوچک باشند تجزیه ی $x+y$ ، $x-y$ به تجزیه ی N می انجامد.

به این منظور x هایی را انتخاب می کنیم که x^2 در مبنا ی N کوچک باشد. برای این کار می توان x را نزدیک $\sqrt{N}$ در نظر گرفت تا $|x^2|$ در مبنای N کوچک باشد. حال اگر $x^2 \cong y^2 \mod N$ که x ، y در مبنای N همنهشت نبودند ، یعنی دوتایی مورد نظر را یافته ایم.

برای مثال برای تجزیه ی $N = 24511$ ابتدا $\sqrt{N} = 156.559..$ را محاسبه می‌کنیم و حال مقادیر x^2 را برای x های نزدیک به $\sqrt{N}$ محاسبه می کنیم.

---

[۱] quadratic sieve

x	$x^2 \pmod N$	Square?
157	138	No
158	453	No
159	770	No
160	1089	Yes (33^2)

پس داریم که $160^2 \cong 33^2 \mod N$ و درنتیجه:

$$24511|(160+33)(160-33) = 193 \times 127$$

متاسفانه در اکثر اوقات پیدا کردن دو مربع به این سادگی نیست. کاری که در عمل انجام می‌دهیم، ضرب تعدادی از این هم‌نهشتی‌ها به این منظور است که دو طرف هم‌نهشتی مربع کامل باشند. به این منظور از حساب اندیسی[۲] استفاده می‌کنیم.

تعریف: عدد N را $B-$ریز [۳] نامیم هرگاه برای هر عدد اول مانند p که $p|N$ داشته باشیم $p \leq B$

حال اگر تعداد زیادی عدد $B-$ریز داشته باشیم می توانیم با اعمال جبر خطی در مبنای ۲ تعدادی از آن‌ها را می‌توان پیدا کرد که ضربشان مربع کامل باشد.

حال از این امر در پیدا کردن جفت مورد نظر استفاده می کنیم. به این منظور دوباره x را حول $\sqrt{N}$ در نظر می گیریم تا x^2 در مبنا ی N کوچک باشد. حال $x^2 - N$ (که عدد کوچکی است) را تجزیه می کنیم و اگر $B-$ ریز بود به مجموعه‌ی X اضافه می کنیم. زمانی که تعداد اعضای X از تعداد اعداد اول کمتر از B بیشتر شد ، می توانیم تعدادی از آن ها را بیابیم که ضربشان مربع کامل است.

برای مثال برای تجزیه ی $N = 227179$ ابتدا $\sqrt{N} = 476.7...$ را محاسبه می کنیم و قرار می دهیم $B = 25$ و $x^2 - N$ را برای اعداد نزدیک $\sqrt{N}$ محاسبه می کنیم و این اعداد را تجزیه می کنیم و اگر $B-$ریز بودند آن ها را به مجموعه‌ی X اضافه می کنیم. مثلا با انتخاب x های در فاصله ی کمتر از 15 از $\sqrt{N}$ داریم :

[۲] index calculus
[۳] B–smooth

x	$x^2 - N$	Factorisation
470	$-$ 6729	$-3 \times 7 \times 13 \times 23$
473	$-$ 3450	$-2 \times 3 \times 5^2 \times 23$
477	350	$2 \times 5^2 \times 7$
482	5145	$3 \times 5 \times 7^3$
493	15870	$2 \times 3 \times 5 \times 23^2$

حال تعدادی را انتخاب می کنیم که ضربشان مربه کامل باشد. مثلا در این مثال

$$(477 \times 482 \times 493)^2 \cong (2 \times 3 \times 5^2 \times 7^2 \times 23)^2 \mod 227179$$
$$477 \times 482 \times 493 \cong 212460 \mod 227179$$
$$، 2 \times 3^2 \times 7^2 \times 23 \cong 169050 \mod 227179$$
$$، (227179, 212460 - 169050) = 1447 ، (227179, 212460 + 169050) = 157 ،$$
$$227179 = 1447 \times 157$$

برای پیاده سازی تجزیه می توان ابتدا اعداد اول کمتر از B را پیدا کرد و سپس اعداد کوچکتر از یک کران مناسب را غربال می کنیم. حال برای پیدا کردن اعدادی که ضربشان مربع کامل است ، یک ماتریس تشکیل می دهیم که سطر ها نماینده ی اعداد $B-$ ریز و ستون ها نماینده ی اعداد اول کمتر از B اند. درایه های ماتریس را اینگونه تعریف می کنیم.

$$M_{n,p} = i \mod 2 \text{ که } p^i || n$$

که اگر تعداد کافی عدد $B-$ ریز بیابیم ، این ماتریس یک جواب صفر کننده ی نا بدیهی دارد که مشخص می کند کدام اعداد باید در هم ضرب شوند.

این الگوریتم در عمل برای اعداد زیر ۱۰۰ رقم ، سریع ترین الگوریتم تجزیه می باشد و ضعف آن در تجزیه ی اعدادی به شکل $N = pq$ که p, q اول اند و فاصله ی آن ها بسیار زیاد می باشد است. برای رفع این مشکل ، قبل از این الگوریتم از الگوریتم های مناسب برای حالت فوق برای در نظر گرفتن این حالت استفاده می شود و سپس غربال مربعی انجام می گیرد .

در قسمت بعد به بررسی الگوریتم غربال میدان عددی که از ایده ی نسبتا مشابه استفاده می کند می پردازیم.

فصل ۳

غربال میدان عددی

غربال میدان عددی [۱] قوی ترین و جامع ترین روش تجزیه ، خصوصا برای اعداد بیش از ۱۰۰ رقم ، تا به امروز است. این الگوریتم از ابزار ها ی نظریه ی جبری اعداد برای انجام عمل تجزیه استفاده می کند. در ابتدا با یک مثال روند کلی این الگوریتم را توضیح می دهیم.

برای مثال عدد $N = 119$ را با این روش تجزیه می کنیم. همانند روش قبل به دنبال پیدا کردن دو عدد x, y هستیم به طوری که $x^2 \cong y^2 \mod N$. اگر دقت کنیم $119 = 11^2 - 2$ و در نتیجه ۱۱ ریشه ی چند جمله ای $x^2 - 2$ در مبنا ی ۱۱۹ است. این به این معنی است که نگاشت زیر یک همریختی حلقه ای است.

$$\phi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}/119\mathbb{Z}$$
$$a + b\sqrt{2} \to a + 11b \mod 119$$

حال با کمی دقت متوجه می‌شویم که

$$\phi(3 + 2\sqrt{2}) = 25 = 5^2$$

و از طرفی

$$.\phi(3 + 2\sqrt{2}) = \phi(1 + \sqrt{2})^2 = 12^2$$

پس

$$5^2 \cong 12^2 \mod 119 \text{ و } (119, 5 + 12) = 17 \text{ ، } (119, 12 - 5) = 7$$

[۱] number field sieve

و در نتیجه

$$119 = 17 \times 7$$

پس مراحل کلی غربال میدان عددی عبارتند از:

۱. انتخاب یک چندجمله ای تحویل ناپذیر و ریشه‌های آن در $\mathbb{C}, \mathbb{Z}/N\mathbb{Z}$

۲. ایجاد همریختی $\phi : \mathbb{Z}[\alpha] \to \mathbb{Z}/N\mathbb{Z}$

۳. پیدا کردن $x \in \mathbb{Z}[\alpha]$ که $\phi(x^2) = y^2$ برای یک $y \in \mathbb{Z}/N\mathbb{Z}$ ، $y \neq \phi(x)$

متاسفانه هیچ یک از مراحل در عمل به سادگی مثال قبل نیستند و چند نمونه از آنها عبارتند از :

۱. پیدا کردن چند جمله ای تحویل ناپذیر و یک ریشه ی آن در مبنا ی N کار ساده ای نیست.

۲. همریختی معرفی شده در واقع از O_K است که $K = \mathbb{Q}(\alpha)$ که لزوما برابر $\mathbb{Z}[\alpha]$ نیست. البته این پدیده در عمل اشکالی ایجاد نمی کند و می توان با محاسبه ی پایه ی صحیح آن را بر طرف کرد.

۳. پیدا کردن عددی مانند $3 + \sqrt{2}$ در حالت کلی راحت نیست. برای این امر نیز از حساب اندیسی کمک می گیریم و سعی به پیدا کردن تعدادی از اعضا می کنیم که ضرب آن ها در شرایط صدق کند. متاسفانه در این الگوریتم اگر پیش‌تصویرها را از مربع کامل‌ها انتخاب کنیم فقط به جواب های بدیهی دست می‌یابیم.

۴. تجزیه در میدان ها ی عددی برای انجام حساب اندیسی کار دشواری است و حتی ممکن است حلقه ی اعداد صحیح میدان عددی فاقد یکتایی تجزیه باشد.

مشکل پیدا کردن چند جمله ای درفصل بعد به طور دقیق بررسی می شود. مشکل اساسی تجزیه ی عناصر حلقه ی اعداد صحیح است.

همان طور که می دانیم حلقه ی ایده آل ها ی O_K همواره دارای خاصیت تجزیه ی یکتا است. در این الگوریتم ما از این خاصیت استفاده می کنیم.

تعریف: عدد جبری α را $B-$ریز نامیم هرگاه برای هر عدد اول p که $p|Norm(\alpha)$ داشته باشیم $p \leq B$.

متاسفانه مربع کامل بودن نرم یک عدد به معنی مربع کامل بودن آن نیست و ما نمی توانیم در حساب اندیسی از نرم به جا ی خود عدد جبری استفاده کنیم. استفاده از ایده آل تولید شده توسط یک عدد جبری انتخاب مناسب تری است. زیرا همان طور که در ادامه گفته میشود ، ایده آل ها قابل تجزیه اند.

همان طور که می دانیم نرم ایده آل های اول توان یک عدد اول است و این عدد خود عضو این ایده آل اول است.(زیرا نرم عضو ایده‌آل است و ایده‌آل اول است.) پس با تجزیه ی ایده‌آل ها ی اصلی به شکل (p) که $p \in \mathbb{P}$ و $p|norm(\alpha)$ می توانیم ایده‌آل های اول شامل α را بیابیم. برای سادگی کار در این قسمت فرض می کنیم که $O_K = Z[\alpha]$ و همچنین $Z[\alpha]$ دارای خاصیت یکتایی تجزیه است.

برای تجزیه ی ایده‌آل ها می توانیم از قضیه ی ددکین_کومر[۲] استفاده کنیم.

قضیه: ایده‌آل های اول حلقه ی اعداد صحیح $\mathbb{Q}(\alpha)$ به شکل $P_{[p,r]} =< p, \alpha - r >$ هستند که $f(r) \cong 0 \mod p$.

برهان: این قضیه نتیجه ی مستقیم قضیه ی ددکین_کومر است.

حال اعداد صحیح اول کوچکتر از B و $P_{[p,r]}$هایی که $p \leq B$ به همراه -1 پایه‌ی تجزیه[۳] را تشکیل می دهند. با داشتن این پایه می توانیم روی اعضای حلقه پیمایش کنیم (چون با در نظر گرفتن پایه صحیح این حلقه یک ریخت با $\mathbb{Z}^k$ است ، می توان این کار را کرد) و سعی می کنیم تعداد زیادی عضو پیدا کنیم که نرم و تصویر آن ها تحت این همریختی $B-$ریز باشد.

پس با اعمال این مراحل $\beta \in O_K$ را طوری می یابیم که،

$$< \beta >=< \beta_{i_1} > \times ... \times < \beta_{i_k} >=< \beta^* >^2$$
$$\phi(\beta) = \phi(\beta_{i_1}) \times ... \times \phi(\beta_{i_k}) = a^2$$

البته چون یکتایی تجزیه را فرض کرده ایم ایده‌آل ها را ایده‌آل اصلی در نظر گرفته ایم.

متاسفانه این موضوع برای اینکه β مربع کامل باشد کافی نیست. زیرا حتی اگر $< \beta >=< \beta^{*2} >$ ممکن است ، $\beta = \lambda\beta^*$ که λ یکه ی حلقه ی O_K است.

مشکلات باقی مانده در این الگوریتم عبارتند از:

[۲] Dedekind–Kummer's factorization theorem
[۳] factor basis

۱. انتخاب چند جمله ای مناسب و ریشه های آن.

۲. حل مشکل عناصر یکه.

۳. بررسی حالتی که O_K دارای یکتایی تجزیه نباشد.

در ادامه به حل دو مورد اول میپردازیم و یک از این الگوریتم برای تجزیه ی عدد 9ام فرما[۴] استفاده می‌کنیم.

[۴] th9 Fermat number

فصل ۴

انتخاب چندجمله ای در غربال میدان عددی

یکی از مشکلات اصلی در غربال میدان عددی انتخاب یک چندجمله ای تحویل ناپذیر p و يك ريشه ي أن در مبنای ،N عدد ورودی الگوریتم تجزیه ، است . پیچیدگی محاسباتی الگوریتم غربال به اندازه ی ضرایب و درجهی چندجمله ای بستگی دارد. پس باید تلاش کرد که چند جمله ای با ضرایب کوچک و درجه‌ی تا حد امکان کوچک یافت.

متاسفانه این امر کار ساده ای نیست . ولی الگوریتم معرفی شده توسط لنسترا در [۴] این مشکل را حل می کند. این الگوریتم در زمان چندجمله ای یک چندجمله ای با ضرایب گویا را به چند جمله ای های تحویل ناپذیر تجزیه می کند.
با داشتن این الگوریتم می توان از هر چندجمله ای در الگوریتم غربال استفاده کرد. زیرا اگر چندجمله ای انتخاب شده تحویل ناپذیر نباشد می توانیم N را به صورت ضرب اعداد کوچکتر بنویسیم که احتمالا تجزیه ی آن ها راحت تر است.

در این بخش به برسی الگوریتم تجزیه چندجمله ای ها با ضرایب گویا می پردازیم.

۱.۴ کاهش پایه در یک مشبکه:

فرض کنید L یک مشبکه n بعدی باشد و $b_1, ..., b_n$ پایه ی L باشد. n را رنک L می‌نامیم و دترمینان $d(L)$ را به این صورت تعریف می‌کنیم

$$d(L) = |det(b_1, ..., b_n)|$$

حال فرض کنید $b_1, ..., b_n$ مستقل خطی باشند ، روش قطری سازی گرام اشمیت را برای b_i ها انجام می دهیم و بردار های b_i^* ، $0 \leq i \leq n$ و اعداد حقیقی μ_{ij} ، $0 \leq i, j \leq n$ را به دست می آوریم.

تعریف: پایه ی $b_1, ..., b_n$ را برای L یک پایه ی کاهش یافته می نامیم هرگاه

$$1 \leq i, j \leq n \text{ ، } \mu_{ij} \leq 1/2$$
$$|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq 3/4 |b_{i-1}^*|^2$$

حال الگریتمی برای به دست آوردن یک پایه ی کاهش یافته از روی یک پایه ی دلخواه معرفی می کنیم.

فرض کنید $b_1, ..., b_n$ یک پایه برای L باشد. ابتدا با استفاده از روش گرام اشمیت b_i و μ_{ij} ها را به دست می آوریم. حال پایه ها را به گونه ای تغییر می دهیم که شرایط تعریف پایه‌ی کاهش یافته را داشته باشند. در ابتدا قرار می دهیم $k = 2$ ، و تلاش کنیم دو شرط زیر برقرار باشند.

$$1 \leq i, j < k \text{ ، } \mu_{ij} \leq 1/2$$
$$1 \leq i < k \text{ ، } |b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq 3/4 |b_{i-1}^*|^2$$

این شرط ها برای $k = 2$ به طور بدیهی برقرار است.

الگوریتم را به صورت استقرایی ادامه می دهیم. اگر $k = n + 1$ پایه کاهش یافته و متوقف می شویم. حال فرض کنید برای $k \leq n$ این شرط برقرار نیست. اگر شرط اول برقرار نباشد فرض کنید r نزدیکترین عدد صحیح به $\mu_{k,k-1}$ باشد. b_k را با $b_k - r b_{k-1}$ جایگزین می کنیم. پس تمام μ_{kj} ها با $j < k - 1$ با $\mu_{kj} - r\mu_{k-1,j}$ جایگزین می شوند و $\mu_{k,k-1}$ با $\mu_{k,k-1} - r$ جایگزین می شود. این کار شرط اول را برقرار می شود.

بعد از این مرحله اگر شرط دوم در k برقرار باشد قرار می دهیم $k = k + 1$ و به ابتدای الگورریتم می رویم. در غیر این صورت b_k و $b_k - 1$ را جابجا می کنیم. با این کار b_{k-1}^* با $b_k^* - \mu_{k,k-1} b_{k-1}^*$ جابه جا میشود و در اندازه اش از $3/4$ اندازه‌ی قبلی‌اش کمتر می‌شود. حال قرار می‌دهیم $k = k - 1$ و الگوریتم را ادامه می‌دهیم. لازم به ذکر است بعد از هر مرحله باید مقادیر b_i^* و $\mu_{i,j}$ را دوباره محاسبه کنیم.

لنسترا در [۴] ثابت کرده این الگوریتم در زمان چندجمله ای متوقف می‌شود و از مرتبه ی زمانی $o(n^4 log(B))$ است که B یک کران بالا برای $|b_i|$ ها باشد.

قضیه: الگوریتمی از مرتبه ی زمانی چند جمله ای وجود دارد که برای عدد صحیح مثبت n و اعداد گویا $\alpha_1, ...\alpha_n, \epsilon$ که $0 < \epsilon < 1$ ، اعداد صحیح $p_1, ..., p_n, q$ را چنان می یابد که

$$1 \leq i \leq n \text{ ، } |p_i - q * \alpha_i| \leq \epsilon$$
$$1 \leq q \leq 2^{n(n+1)/4}\epsilon^{-n}$$

طرح اثبات: برای پیدا کردن p_i ها و q ستون ها ی ماتریس زیر را به عنوان پایه های یک مشبکه از رنک $n+1$ در نظر می گیریم و الگوریتم کاهش را اعمال می کنیم.

$$\begin{pmatrix} 1 & 0 & \dots & 0 & -\alpha_1 \\ 0 & 1 & \dots & 0 & -\alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -\alpha_n \\ 0 & 0 & \dots & 0 & 2^{-n(n+1)/4}\varepsilon^{n+1} \end{pmatrix}.$$

حال می توانیم بنویسیم

$$b_1 = (p_1 - q\alpha_1, ..., q.2^{n(n+1)/4}e^{n+1})$$

که b_1 اولین بردار پایه‌ی کاهش یافته است و این p_i ها و q در شرایط خواسته شده صدق می کند.

از الگوریتم کاهش پایه می توان برای پیدا کردن رابطه های Qـخطی بین اعداد حقیقی $\alpha_1, ..., \alpha_n$ استفاده کرد. برای این کار شبکه ی خود را $\mathbb{Z}^n$ انتخاب می‌کنیم و آن را به روش زیر در $\mathbb{R}^{n+1}$ می‌نشانیم.

$$(m_1, m_2, ..., m_n) \to (m_1, m_2, m_3, ..., c\sum_{i=1}^{n} m_i\alpha_i^{'})$$

که در آن c یک ثابت بزرگ و $\alpha_i^{'}$ یک تقریب خوب از α_i است. که اگر پایه ی کاهش یافته ی شبکه را در نظر بگیریم به ما $m_1, ..., m_n$ را طوری می دهند که $\sum_{i=1}^{n} m_i\alpha_i^{'}$ بسیار کوچک باشند. اگر برای یک عدد حقیقی α تعریف کنیم $\alpha_i = \alpha^{i-1}$ می توان از روش قبل برای محک جبری بودن یک عدد استفاده کرد.

حال از این الگوریتم برای تجزیه ی چندجمله ای ها کمک می گیریم.

۲.۴ تجزیه ی چند جمله ای ها

در کل این بخش در نظر بگیرید که f یک چندجمله ای در $\mathbb{Z}[X]$ با درجه ی $n > 0$ است و $h \in \mathbb{Z}[X]$ خواص زیر را دارا است.

۱. h ضریب پیشرو ۱ دارد.

۲. $f(mod(p^k)) \mid h(mod(p^k))$ در $(\mathbb{Z}/p^k\mathbb{Z})[X]$

۳. h در $(\mathbb{Z}/p\mathbb{Z})[X]$ تحویل ناپذیر است.

۴. h با توان یک در تجزیه ی f در $(\mathbb{Z}/p\mathbb{Z})[X]$ ظاهر می شود.

قرار می دهیم $l = deg(h)$ پس $l \leq n$.

قضیه: چند جمله ای f دارای یک عامل مانند $h_0 \in Z[X]$ است به طوری که $g(mod(p)) \mid h(mod(p))$ و این عامل با صرف نظر از علامت به طور یکتا تعین می گردد.

برای اثبات این قضیه به [۴] مراجعه کنید.
در ادامه ی این قسمت عدد طبیعی m را ثابت در نظر گرفته و شبکه‌ی L را تصویر تمام چند جمله ای های با ضرایب صحیح از درجه ی حداکثر m با نگاشت زیر در نظر می گیریم که در $(Z/p^kZ)[X]$ به $h(mod(p^k)$ بخش‌پذیرند.

$$\sum_{i=0}^{m} a_i X^i \to (a_0, a_1, ..., a_n)$$

و بدیهی است که

$$\{p^k X^i : 0 \leq i < l\} \cup \{hX^j : 0 \leq j \leq m - l\}$$

و در نتیجه داریم $d(L) = p^{kl}$.

حال f ، h، p ، k را به همین صورت در نظر بگیرید. و فرض کنید ضرایب h در مبنای p^k کاهش یافته‌اند و در نتیجه

$$|h|^2 \leq 1 + lp^{2k}$$

و حال فرض کنید $m \geq l$ داده شده است که نامساوی زیر برقرار باشد.

$$p^k l > 2^{mn/2} . \binom{2m}{m}^{n/2} . |f|^{m+n}$$

حال الگوریتمی را معرفی می کنیم که مشخص می کند در صورت وجود h_0 آیا درجه ی آن از m کمتر است یا خیر و اگر کمتر بود h_0 را مشخص می کند.برای انجام این کار به قضیه ی زیر نیاز مندیم.

قضیه: با فرض تعریف این بخش اگر $b_1, ..., b_{m+1}$ یک پایه ی کاهش یافته برای L باشد و نا مساوی ،

$$p^k l > 2^{mn/2}.\binom{2m}{m}^{n/2}.|f|^{m+n}$$

برقرار باشد ، آنگاه داریم که $deg(h_0) \leq m$ اگر و تنها اگر $|b_1| < (p^{kl}/|f|^m)^{1/n}$.

برای مشاهده ی اثبات قضیه به [۴] مراجعه کنید.

حال با داشتن قضیه ی فوق می توان با استفاده از الگوریتم کاهش پایه ، الگوریتم مورد نظر را طراحی کنیم.

به این منظور پایه ی $\{p^k X^i : 0 \leq i < l\} \cup \{hX^j : 0 \leq j \leq m - l\}$ را در نظر می گیریم و پایه ی کاهش یافته ی $b_1, b_2, ...b_{m+1}$ را به دست می آوریم.
حال طبق قضیه ی قبل اگر $|b_1| \geq (p^{kl}/|f|^m)^{1/n}$ نتیجه می گیریم که $deg(h_0) > m$.
در غیر این صورت برای پیدا کردن h_0 از قضیه ی زیر کمک می گیریم.

قضیه: با توجه به نماد ها و تعریف این بخش ، اگر فرض کنیم اندیس $1 \leq j \leq m + 1$ چنان موجود باشد که

$$|b_j| < (p^{kl}/|f|^m)^{1/n}$$

و t بزرگترین این اندیس ها باشد، داریم که

$$deg(h_0) = m + 1 - t$$
$$h_0 = gcd(b_1, ..., b_t)$$

برای اثبات این قضیه به [۴] مراجعه نمایید.

با داشتن این قضیه اگر $|b_1| \geq (p^{kl}/|f|^m)^{1/n}$ درجه ی h_0 کمتر از m است و

$$h_0 = gcd(b_1, ..., b_t)$$

که t در قضیه معرفی شده.

برای محاسبه ی $gcd(b_1, ...b_t)$ از الگوریتم $subresultant$ که در [۳] معرفی شده استفاده می کنیم.

تجزیه ی یک چند جمله ای در مبنای p کار ساده‌ای است. پس می توانیم h ها را بیابیم و با تغییر m ، h_0 را بیابیم و در نتیجه می توان چند جمله ای دلخواه f را به عوامل تحویل نا پذیر تجزیه کرد. و لنسترا در[۴] ثابت کرده که تمامی مراحل در زمان چند جمله ای انجام می گردد پس این الگوریتم از مرتبه زمانی چندجمله ای است.

با داشتن این الگوریتم نیازی به انتخاب چندجمله ای تحویل نا پذیر در الگوریتم غربال میدان عددی نیست. زیرا تجزیه ی این چند جمله ای ، که در زمان چند جمله ای ممکن است ، منجر به تجزیه ی عدد N می شود و به این دلیل حالتی که f تحویل ناپذیر نباشد ، مشکلی ایجاد نمی کند.

فصل ۵

تجزیه ی F_9 به کمک غربال میدان عددی

متاسفانه استفاده از غربال میدان عددی در خیلی مواقع کار بسیار دشواری است. مشکلاتی چون عدم برقراری یکتایی تجزیه و دشواری محاسبه ی یکه ها از این قبیل اند. با این حال در بعضی مواقع این مشکلات قابل حل هستند.

اگر در حلقه ی انتخاب شده یکتایی تجزیه وجود داشته باشد و یکه های پایه [۱] به راحتی قابل مقایسه باشند ، با افزودن چند ستون به ماتریس ساخته شده در مرحله ی حساب اندیسی می توان این مشکلات را حل کرد.

یکي از نمونه هایی که این حالت اتفاق می افتد تجزیه ی عدد ۹ام فرما است. برای تجزیه ی F_9 از حلقه ی $\mathbb{Z}[\sqrt[5]{2}]$ استفاده می کنیم حال به بررسی خواص این حلقه می پردازیم. نگاشت در نظر گرفته شده در این بخش به شرح زیر است.

$$\phi : \mathbb{Z}[\sqrt[5]{2}] \to \mathbb{Z}/N\mathbb{Z}$$
$$\phi(\sqrt[5]{2}) = 2^{205} \mod N$$

۱.۵ تابع نرم:

اعضای میدان $\mathbb{Q}(x)$ به طور یکتا به شکل $\sum_{i=0}^{4} q_i \sqrt[5]{2}^i$ نمایش داد که $q_i \in \mathbb{Q}$. ضرب یک عنصر از میدان در $\beta = \sum_{i=0}^{4} q_i \sqrt[5]{2}^i$ همانند این است که بردار متناظر آن را در ماتریس زیر است.

[۱] fundamental units

$$\begin{pmatrix} q_0 & 2q_4 & 2q_3 & 2q_2 & 2q_1 \\ q_1 & q_0 & 2q_4 & 2q_3 & 2q_2 \\ q_2 & q_1 & q_0 & 2q_4 & 2q_3 \\ q_3 & q_2 & q_1 & q_0 & 2q_4 \\ q_4 & q_3 & q_2 & q_1 & q_0 \end{pmatrix}$$

پس نرم β برابر دترمینان این ماتریس است.
به طور خاص داریم که $N(a - b\sqrt[5]{2}^i) = a^5 - 2^i b^5$.

۲.۵ ایده‌آل ها:

قضیه: $Z[\sqrt[5]{2}]$ یک حوزه‌ی ایده‌آل اصلی است.

خلاصه‌ی برهان: برای اثبات این قضیه ثابت می کنیم عدد رده ای[۲] این حلقه 1 است واین امر با استفاده از ثابت مینکفسکی[۳] انجام می شود.در این حلقه $M = 13$. است و این به این معنی است که فقط ایده آل های با نرم کمتر از ۱۳ را بررسی کنیم. این امر نیز با تجزیه ی ایده آل ها ی اصلی اعداد اول کمتر مساوی ۱۳ ممکن است.

پس تا به اینجا مشکلی در انجام غربال وجود ندارد. مرحله ی بعدی پیدا کردن یکه های این حلقه می باشد.

۳.۵ محاسبه ی یکه ها:

قضیه‌ی دیریشله برای یافتن یکه‌های مقدماتی به ما کمک می‌کند. طبق این قضیه $\mathbb{Z}[\sqrt[5]{2}]^*$ [۴] توسط دو عنصر یکه از مرتبه ی نا متناهی به همراه -1 گروه یکه ها را تولید می کند. دو یکه ی مستقل ضربی و با مرتبه ی نا متناهی در $\mathbb{Z}[\sqrt[5]{2}]$ عبارتند از.

[۲] class number
[۳] Minkowski constant
[۴] the unit group of $\mathbb{Z}[\sqrt[5]{2}]$

$$\epsilon_0 = -1$$
$$\epsilon_2 = -1 + \sqrt[5]{2}^2 + \sqrt[5]{2}^3 + \sqrt[5]{2}^4 \text{ ، } \epsilon_1 = -1 + \sqrt[5]{2}$$

حال داریم که برای هر $\epsilon \in Z[\sqrt[5]{2}]^*$ می توانیم بگوییم ، $\epsilon = \epsilon_0^{v(0)} \times \epsilon_1^{v(1)} \times \epsilon_2^{v(2)}$.

۴.۵ تجزیه:

یک عامل F_9 قبل از پیدایش غربال میدان عددی محاسبه شده بود و آن $p_7 = 2424833$ بود.
پس قرار می دهیم $n = F_9/2424833$ و $\phi : \mathbb{Z}[\sqrt[5]{2}] \to \mathbb{Z}/n\mathbb{Z}$ را به شکل $\phi(\sqrt[5]{2}) = 2^{205}$ تعریف میکنیم. اگر به $\alpha = \sqrt[5]{2}^3$ دقت کنیم و ، $\phi(\alpha) = 2^{103}$ که به نسبت n بسیار کوچک است. به همین دلیل در الگوریتم غربال اعضای به شکل $a + b\alpha$ را پیمایش می کنیم.

کران β را برابر 1295377 در نظر گرفته می شود و سه یکه ی پایه ی معرفی شده به پایه تجزیه ی جبری اضافه می شوند.
با پیاده سازی این الگوریتم ثابت شد که $F_9 = p_7 \times p_{49} \times p_{99}$ است که ،

$p_7 = 2424833$
$p_{49} = 74556028256478842083373957362004549187833663426 57$
$p_{99} = 74164006262753080152478714190193747405994078109751902 39$
$05821316144415759504705008092818711693940737$

متاسفانه الگوریتم غربال میدان عددی برای تجزیه ی همه ی اعداد به این خوشرفتاری نیست و حالت کلی آن قابل پیاده سازی نیست. زیرا مراحل آن ،به خصوص انتخاب چند جمله ای و یافتن یکه ها بسیار وابسته به عدد ورودی الگوریتم هستند.

با این حال این الگوریتم ، با وجود مرتبه زمانی نمایی و مشکلات پیاده سازی سریع‌ترین الگوریتم تجزیه تا به امروز می باشد.

۵.۵ مشکل یکه‌ها در حالت کلی:

در این بخش به بررسی نحوه‌ی یافتن یکه‌های مقدماتی در تجزیه‌ی F_9 پرداختیم ولی نحوه‌ی یافتن ϵ_1, ϵ_2 این دو یکه مشخص نشد و ممکن است در حالت کلی یافتن یکه‌ها یه این سادگی نباشد. در این بخش به معرفی یک روش برای یافتن این یکه‌ها می پردازیم.

فرض کنید O حلقه‌ی اعداد صحیح جبری میدان عددیK باشد و $\theta_1, ..., \theta_n$ نشاندن‌های این حلقه در $\mathbb{C}$ باشند. طبق قضیه دریشله ، تابع

$$Log : K - \{0\} \to \mathbb{R}^n$$
$$Log(\alpha) = (\log|\theta_1(\alpha)|, ..., \log|\theta_n(\alpha)|)$$

یک هومومرفیسم ضرب به جمع است و کرنل آن $TU(O)$ است که مولدهای آن ریشه‌های چندجمله‌ای متقارن $\phi_{w(O)}(t) = \prod_{1\leq d|w(O)}(t^d - 1)^{\mu(w(O)/d)}$ اند. که با روش معرفی شده در [۶] قالبل محاسبه‌اند.
و داریم که

$$U(O) = ker(Log) \times < \eta_1 > \times ... \times < \eta_r >$$

پس باید یکه‌های $\epsilon_1, ...\epsilon_r$ را چنان بیابیم که مستقل خطی باشند. روشی که معرفی خواهیم کرد توسط مینکفسکی معرفی شده.

تعریف: اگر $w = \sum_{i=0}^{n} \beta_i w_i \in O$ ، تعریف می‌کنیم

$$l_3(w) = (\beta_1, ..., \beta_n)$$

تعریف: اگر $L = \sum_{i=1}^{p} \mathbb{Z}v_i$ یک مشبکه باشد ، تعریف می کنیم

$$\prod(v_1, ..., v_p) = \{\sum_{i=1}^{p} \beta_i v_i | -1/2 \leq \beta_i \leq 1/2\}$$

$$\prod(w) = 2\prod(l_3(w_1), l_3(w_2), ..., l_3(w_n))$$

الگوریتم: اگر $r = 0$ که داریم $U(O) = TU(O)$ و گفته شد که مولدهای این گروه قابل محاسبه‌اند. حال فرض کنید p یکه‌ی مستقل خطی $\epsilon_1, ..., \epsilon_p$ و اعضای غیر برابر $\omega_1, ..., \omega_{\alpha(p)} \in O$ را تا به حال به دست آورده‌ایم به طوری که

$$\alpha(p) > 0 \text{ ، } 0 \leq p \leq r$$

$$x \in \prod(w) \text{ ، } |\omega_i| \leq |N_{l_3}(x)|$$

حال $w \in O$ را انتخاب می‌کنیم شبکه‌ی $\prod(w)$ را تشکیل می دهیم و نقاط این شبکه را می یابیم. فرض کنید $\pm\phi_1, ... \pm \phi_k$ باشند.
اگر یکی از ϕ_i/ω_j ها یکه باشد ، آن را به ϵ_i ها اضافه می‌کنیم و $\epsilon_1^{'}, ..., \epsilon_{p'}^{'}$ را طوری می‌یابیم که زیرگروه یکسانی با $\{\epsilon_1, ..., \epsilon_p\} \cup \{\phi_i/\omega_j\} \cup TU(O)$ بسازد و $\epsilon_i^{'}$ ها مستقل خطی باشند.
حال $\epsilon_1, ..., \epsilon_p$ را با $\epsilon_1^{'}, ..., \epsilon_{p'}^{'}$ عوض می کنیم. اگر $p^{'=r}$ که پایه را یافته‌ایم. در غیر این صورت قرار می دهیم $\omega_{\alpha(p)+1} = \phi_i$ و دوباره این الگوریتم را اجرا می‌کنیم و اگر برای همه‌ی ϕ_i ها تکرار کردیم w را تغییر می‌دهیم.

برای اثبات اینکه این الگوریتم پایان‌پذیر است به [۶] مراجعه نمایید.

این الگوریتم با اینکه همواره یکه‌های اولیه را می یابد ، پیچیدگی محاسباتی معینی ندارد و به دلیل زمان اجرای زیاد ، برای استفاده در غربال مربعی مناسب نمی‌باشد. به همین دلیل تا به امروز غربال مربعی فقط در حلقه‌هایی استفاده شده که محاسبه‌ی یکه‌های آن‌ها ساده است.

واژه‌نامه فارسی به انگلیسی

عدد جبری algebraic number
میدان عددی number field
عدد صحیح جبری algebraic integer
پایه صحیح integral basis
نرم norm
نشاندن embedding
ایده‌آل اصلی principal ideal
حوزه‌ی تجزیه‌ی یکتا uniform factorization domain
ایده‌آل کسری fractional ideal
عدد رده‌ای class number
گروه رده‌ای class group
کلید عمومی public key
کلید خصوصی private key
غربال sieve
غربال مربعی quadratic sieve
حساب اندیسی index calculus
غربال میدان عددی number field sieve
یکه‌های پایه fundamental unit
مشبکه‌اشبکه lattice

کتاب‌نامه

[1] Henri Cohen, *A Course in Computational Algebraic Number Theory*

[2] F. Jarvis , *Algebraic Number Theory*

[3] D. E. Knuth , *the art of computer programming Vol. 2*

[4] A. K. Lenstra , H. W. Lenstra Jr. , L. Lovasz , *Factoring Polynomials With Rational Coefficients*

[5] A. K. Lenstra , H. W. Lenstra Jr. , J. M. Pollard *The factorization of the 9th fermat number*

[6] H. Zassenhaus , *On Hensel factorization. I*

Abstract

The word sieve is a utensil consisting of a wire or plastic mesh held in a frame, used for straining solids from liquids, for separating coarser from finer particles, or for reducing soft solids to a pulp. It was first used in number theory by Eratosthenes for classifying primes number's less than a bound B.

The main idea of the algorithm given by Eratosthenes was later used in many factorization methods , called the sieve algorithms. One of the most recent algorithms using this idea is the Number Field Sieve(NFS) which carries the idea of the standard sieve algorithm while using some help from algebraic number theory tools.

In this report we'll define the algorithm give some more in depth explanation about the problems and difficulties arose while implementing this method and explain some methods proposed to solve this difficulties. In the final section we'll explain how the algorithm was used to factorize the 155 digit integer F_9 , the 9th fermat number.

College of Science
School of Mathematics, Statistics, and Computer Science

The number field sieve and modern factorization methods

Khashayar Barooti

Supervisor: Dr. Amir Ghadermarzi

A thesis submitted to Graduate Studies Office
in partial fulfillment of the requirements for the degree of
B.Sc. in
Computer Science

Summer 2017