Глава 9

Разлагане на прости множители

В тази глава ще опишем четири съвременни метода за разлагане на цели числа в произведение от множители, а именно метода на верижните дроби, квадратичното решето, number field sieve и методите на Polard. Всичките методи се основават на следната идея:

Нека N е числото, което трябва да се разложи. Търсим цели числа x и y, такива че

$$x^2 \equiv y^2 \pmod{N} \quad x \not\equiv \pm y.$$

Ако те съществуват, то намираме най-големите общи делители $(x+y, N)$ и $(x-y, N)$. Поне единият от тях трябва да е нетривиален множител на N, тъй като $N|(x^2 - y^2)$.

Идеята за намиране на x и y се състои в намиране за различни естествени k на конгруенции от вида

$$x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} p_2^{e_{2k}} \dots p_m^{e_{mk}} \pmod{N},$$

където p_i са "малки" прости числа от някаква отнапред зададена база, а e_{ik}

Решаваме над $\mathbb{Z}_2$ линейната система

$$\sum_{1 \le k \le n} \epsilon_k (e_{1k}, e_{2k}, \dots, e_{mk})^\tau = (0, 0, \dots, 0)^\tau$$

относно $(\epsilon_1, \dots, \epsilon_n)$ и полагаме

$$x = \prod_{1 \le k \le n} x_k^{\epsilon_k}, \qquad y = (-1)^{v_0} p_1^{v_1} p_2^{v_2} \dots p_m^{v_m},$$

където

$$2(v_0, v_1, \dots, v_m)^\tau = \sum_{1 \le k \le n} \epsilon_k (e_{1k}, e_{2k}, \dots, e_{mk})^\tau.$$

9.1 Метод на верижните дроби

Нека N е числото, което трябва да се разложи, а k е естествено число такова, че $kN \equiv 0$ или $1 \pmod 4$. Фиксираме някаква база от "малки" прости числа. $\sqrt{kN}$ се развива във верижна дроб, като приближените ѝ дроби

$$[a_0; a_1, a_2, \dots, a_n] = \frac{P_n}{Q_n}$$

са добри приближения на $\sqrt{kN}$ дори за малки n. В такъв случай $t = P_n^2 - Q_n^2 kN$ е относително малко и може да се разложи като се използва избраната база от прости числа. След това прилагаме описания в началото на настоящата глава метод за намиране на $x^2 \equiv y^2 \pmod N$.

Развитието на $\sqrt{kN}$ получаваме с алгоритъма описан в параграф 1.5. Да напомним, че рекурентната връзка за (P_n, Q_n) се дава с

$$(P_n, Q_n) = a_n(P_{n-1}, Q_{n-1}) + (P_{n-2}, Q_{n-2}), \quad (P_{-1}, Q_{-1}) = (1, 0),\ (P_0, Q_0) = (a_0, 1).$$

Пример 9.1.1 Нека $N = 7957$. Прилагайки алгоритъма от параграф 1.5 получаваме последователно $a_0 = \lfloor\sqrt{7957}\rfloor = 89$, $a_1 = 4,\ a_2 = 1, \ldots$, а за приближените дроби

n	0	1	2	3	4
P_n	89	357	446		
Q_n	1	4	5		
t	-36	137	-9		

Следователно $(446.89)^2 \equiv (-6^2)(-9) \pmod{7957}$

От сравнението получаваме $\gcd(446.89 - 18, 7957) = 109$ и $\gcd(446.89 + 18, 7957) = 73$ Следователно

$$7957 = 109.73$$

/ Да отбележим, че $(-1)^n t_n = P_{n-1}^2 - Q_{n-1}^2 D$, където t_n е от алгоритъма в параграф 1.5 /

9.2 Метод на квадратичното решето

9.2.1 Метод на Гаус

Този подход е в основата на много от съвременните методи от тип "решето".

Фиксираме множество (наричано *база*) от прости числа ненадминаващи някаква горна граница $\{p_1, p_2, \ldots, p_n\}$. За $k = 1, 2, \ldots$ изчисляваме $x_k = \lfloor\sqrt{kN}\rfloor$ и $a_k = x_k^2 - kN$. Очевидно $x_k \equiv a_k \pmod N$. Числата a_k са обикновено малки и с проверка се разлагат в произведение на прости числа от базата (тези, които съдържат делители извън базата се изключват от разглеждане). Намираме числа, такива че произведението им $b^2 = a_{k_1} a_{k_2} \ldots a_{k_t}$ да е точен квадрат. Нека $x = x_{k_1} x_{k_2} \ldots x_{k_t}$. Тогава

$$x^2 \equiv b^2 \pmod N \qquad \Longrightarrow \qquad N \mid (x - b)(x + b)$$

Следователно $\gcd(N, x - b)$ и $\gcd(N, x + b)$ евентуално ще дадат делител на N.

Обикновенно заедно с a_k се пресмята и $b_k \equiv (x_k + 1)^2 \pmod N$.

Пример 9.2.1 Нека $N = 13843$. Изчислявайки x_k и $x_k + 1$ за $k = 1, 2, \ldots, 10$:

x_k	117	118	166	167	203	204	235	236	263	264
a_k	-154	81	-130	203	-320	87	-147	324	-46	481
x_k	288	289	311	312	332	333	352	353	372	373
a_k	-114	463	-180	443	-520	145	-683	22	-46	699

От горната таблица веднага се вижда, че $118^2 \equiv 9^2 \pmod{13843}$, т.е. $13843 \mid (118 - 9)(118 + 9) = 127.109$. Лесно се вижда, че $13843 = 109.127$.

От таблицата веднага се вижда и че $(263.372)^2 \equiv 46^2 \pmod{13843}$ Тогава $\gcd(263.372-46, 13843) = 127$, откъдето също получаваме разлагането на 13843.

9.2.2 Базисен метод

При този метод се разглежда $x = \lfloor\sqrt{kN}\rfloor + a$, където a приема цели стойности в някакъв интервал около нулата, а не само 0 и 1. Това се прави, обаче, за една или само няколко стойности на k.

За всяко a от разглеждания интервал се изчислява

$$Q(a) = \left(\lfloor\sqrt{kN}\rfloor + a\right)^2 - kN.$$

Ясно е, че $x = \lfloor\sqrt{kN}\rfloor + a$ удовлетворява желаното от нас сравнение $x^2 \equiv Q(a) \pmod{N}$, като при това $Q(a)$ не трябва да е много голямо за да може да се разложи ползвайки базата от прости числа. (При $a = O(N^\epsilon)$ имаме $Q(a) = O(N^{1/2+\epsilon})$). Ако числото $Q(a)$ (или произведение на такива числа получени за няколко различна a) е точен квадрат, то ще получим търсеното сравнение по модул N между два квадрата.

Не за всички a числото $Q(a)$ ще се дели на просто число от избраната база. Наистина нека $m = p^t,\ t = 1, 2, \ldots,$ и $y^2 \equiv kN \pmod{m}$. Тогава $Q(a) = x^2 - kN \equiv x^2 - y^2 \pmod{m}$. Следователно

$$Q(a) \equiv 0 \pmod{m} \qquad \Longleftrightarrow \qquad x^2 \equiv y^2 \pmod{m}, \quad \text{т.е.} \quad x \equiv y \pmod{m}.$$

(y приема две стойности различаващи се по знак)

Следователно

$$a + \lfloor\sqrt{kN}\rfloor \equiv y \pmod{m} \quad \text{т.е.} \quad a \equiv y - \lfloor\sqrt{kN}\rfloor \pmod{m}$$

за всяко решение на $y^2 \equiv kN \pmod{m}$. Последното има решение тогава и само тогава, когато

$$\left(\frac{kN}{p}\right) = 1.$$

Ако $p = 2$, то $N \equiv 1 \pmod{8}$ за $t \geq 3$ или $N \equiv 1 \pmod{4}$.

Наблюдението, че $m \mid Q(a)$ влече $m \mid Q(a + lm)$ за произволно цяло l ни позволява да разширяваме полученото множество от стойности a, за които $m \mid Q(a)$.

В конкретна реализация на алгоритъма въпрос на преценка (и експерименти) е дали да се пресмятат и разлагат $Q(a)$ за всички a в разглеждания интервал или да се пресяват чрез символа на Льожандър.

Пример 9.2.2 Нека $N = 91$. $\lfloor\sqrt{91}\rfloor = 9$. Числото $91 \not\equiv 1 \pmod{4}$, така че $p = 2$ отпада. Нека $m = 3^2 = 9$. $x^2 \equiv 91 \equiv 1 \pmod{9}$ има за решение $x = 1$ и $x = -1 \equiv 8 \pmod{9}$. В такъв случай $a = 1 - 9 \equiv 1 \pmod{9}$ и $a \equiv -1 \pmod{9}$. Тогава $Q(1) = 9 = 3^2$, $Q(-1) = -27$, което дава $(1 + 9)^2 \equiv 3^2 \pmod{91}$. Следователно $91 \mid (10 - 3)(10 + 3)$, откъдето $91 = 7.13$

Пример 9.2.3 Нека $N = 7957$. В базата включваме $m_1 = 2^k, k = 1, 2,\ m_2 = 3^k$, и $m_3 = 11^k$, тъй като $\left(\frac{7957}{p}\right) = 1$, за $p = 3,\ 11$. Пресмятаме $\lfloor\sqrt{7957}\rfloor = 89$. Сравнението $x^2 \equiv 7957 \pmod 4$ има за решение $x = \pm 1$, което дава $a = x - 89 \equiv 0$ или $2 \pmod 4$. Сравнението $x^2 \equiv 7957 \pmod 9$, т.е. $x^2 \equiv 1 \pmod 9$ има за решение $x = \pm 1$. Това води до $a = x - 89 \equiv 0$ или $2 \pmod 9$. Да изчислим $Q(0) = -36 = -6^2$ и $Q(2) = 324 = 2^2.9^2$. Стойността $Q(2)$ е точен квадрат и ще свърши работа. Тя отговаря на $x = 91 = 89 + 2$ и затова имаме $91^2 \equiv 18^2 \pmod{7957}$, т.е. $(91 + 18)(91 - 18) \equiv \pmod{7957}$. Следователно 7957=109.73

9.2.3 Модифициран метод (Multiple Polynomial Quadratic Sieve)

Този метод е по идея на P. Montgomery, който предлага $Q(a)$ да се замени с множество различни квадратни тричлени, такива че

$$Q(x) = Ax^2 + 2Bx + C, \quad A > 0,\ D = B^2 - AC > 0,\ N \mid D$$

При така избраните коефициенти е изпълнено

$$AQ(x) = (Ax + B)^2 - D \equiv (Ax + B)^2 \pmod N.$$

Обикновенно се взема $D = N$ за да запазим по-малки стойностите на Q и коефициентите му.

Ако искаме да "пресеем" $Q(x)$ в интервал с дължина $2M$, то е естествено да го вземем с център $-\frac{B}{A}$, където тричлена достига минимума $-\frac{D}{A}$, т.е.

$$I = \left[-\frac{B}{A} - M,\ -\frac{B}{A} + M\right].$$

За да не надхвърля абсолютната стойност на $Q(x)$ числото N искаме $Q(-\frac{B}{A}) \approx Q(-\frac{B}{A} + M)$, което влече $AM^2 \approx 2D = 2N$. Следователно

$$A \approx \frac{\sqrt{2N}}{M}$$

и за така избраното A е в сила

$$\max_{x \in I} |Q(x)| \approx \frac{N}{A} \approx M\sqrt{N/2}$$

За така избраното A трябва да определим B, C, така че $D = B^2 - AC = N$. Последното става като решаваме сравнението

$$B^2 \equiv N \pmod A \qquad \text{и определяме} \qquad C = \frac{B^2 - N}{A}.$$

За да си осигурим съществуване на решение B избираме

$$\text{просто} \quad A \approx \frac{\sqrt{2N}}{M} : \quad \left(\frac{N}{A}\right) = 1.$$

Пример 9.2.4 Нека $N = 13\,843$ и $M = 10$. Тъй като $\sqrt{2N} \approx 166,4$, то търсим $A = 17, 19, \ldots$. Но

$$\left(\frac{13843}{17}\right) = \left(\frac{5}{17}\right) = \left(\frac{2}{5}\right) = -1$$

докато

$$\left(\frac{13843}{19}\right) = \left(\frac{11}{19}\right) = -\left(\frac{2}{11}\right) = 1.$$

Затова вземаме $A = 19$, откъдето $B^2 \equiv 13843 \equiv 11 \pmod{19}$, т.е. $B \equiv \pm 7 \pmod{19}$ и $C = -726$. Следователно

$$Q_{1,2}(x) = 19x^2 \pm 14x - 726 \qquad \text{и } 19Q_{1,2}(x) \equiv (19x \pm 7)^2 \pmod{13843}.$$

$Q_1(-10)$	$Q_1(-9)$	$Q_1(-8)$	$Q_1(-7)$	$Q_1(-6)$	$Q_1(-5)$	$Q_1(-4)$	$Q_1(-3)$	$Q_1(-2)$	$Q_1(-1)$
1034	687	378	107	-126	-321	-478	-597	-678	-721
$Q_1(0)$	$Q_1(1)$	$Q_1(2)$	$Q_1(3)$	$Q_1(4)$	$Q_1(5)$	$Q_1(6)$	$Q_1(7)$	$Q_1(8)$	$Q_1(9)$
-726	-693	-622	-513	-366	-181	42	303	602	939

$Q_1(-8)Q_1(6) = 378.42 = 2^2.3^4.7^2$ е точен квадрат. Следователно

$$(-145)^2 121^2 = (19.(-8) + 7)^2(19.6 + 7)^2 \equiv 19^2 Q_1(-8)Q_1(6) = 2394^2 \pmod{13843}, \text{т.е.}$$

$$15151.19939 = (17545 - 2394)(17545 + 2394) \equiv 0 \pmod{13843}.$$

Следователно 13843 има общ множител с всяко от 15151 и 19939. Наистина

$$(15151, 13843) = 109, \qquad (19939, 13843) = 127 \qquad \text{и} \qquad 109.127 = 13843.$$

Следващото просто число p с $\left(\frac{13843}{p}\right) = 1$ е 43. Тогава $A = 43$, $B^2 \equiv 13843 \equiv 40 \pmod{43} \Rightarrow B = 13$, $C = (13^2 - 13843)/43 = -318$ и

$$Q(x) = 43x^2 + 26x - 318, \qquad 43Q(x) \equiv (43x + 13)^2 \pmod{13843}.$$

$Q(-10)$	$Q(-9)$	$Q(-8)$	$Q(-7)$	$Q(-6)$	$Q(-5)$	$Q(-4)$	$Q(-3)$	$Q(-2)$	$Q(-1)$
3722	2931	2226	1607	1074	627	266	-9	-198	-301
$Q(0)$	$Q(1)$	$Q(2)$	$Q(3)$	$Q(4)$	$Q(5)$	$Q(6)$	$Q(7)$	$Q(8)$	$Q(9)$
-318	-249	-94	147	474	887	1386	1971	2642	3399

Оставяме на читателя да провери, че с получените стойнсти не може да получим разлика на квадрати.

Ако вземем $p = 11$ тогава $Q(x) = 11x^2 + 8x - 1257$, $11Q(x) \equiv (11x+4)^2 \pmod{13843}$. За $x = -11$ и $x = 3$ се получават стойности, които може да използваме и да разложим 13843.

Нека B_0 е минималното решение на $B^2 \equiv N \pmod{A}$ при фиксирано A и $Q_0(x) = Ax^2 + 2B_0x + C_0$. Всяко $B_k = B_0 + kA$ е също решение и с него може да се изчисли $C_k = C_0 + 2kB_0 + k^2A$ и състави $Q_k(x)$. Но лесно се проверява, че

$$Q_k(x) = Q_0(x + k)$$

Следователно няма смисъл това да се прави, за фиксирано A се вземат само $Q(x) = Ax^2 \pm B_0 x + C_0$.

За всяка степен p^k на простите числа от базата решаваме $u^2 \equiv N \pmod{p^k}$ и със стойностите $(-B+u)/A$ също може да се инициализира ситото. Наистина

$$AQ\left(\frac{-B+u}{A}\right) = u^2 - N \equiv 0 \pmod{p^k}.$$

Следователно и

$$Q\left(\frac{-B+u}{A}\right) \equiv 0 \pmod{p^k}.$$

При използване на разгледаните методи важна роля играе избраната база, т.е. колко големи прости числа p_i да разглеждаме. Тук няма да дискутираме този проблем, но една горна граница, която можже да се намери в литературата е

$$B \approx \exp\left(\frac{1}{2}\sqrt{(\ln\ln N - \ln 2)\ln N}\right).$$

9.3 Методи на John M. Pollard

9.3.1 Метод Pollard p-1

Нека p е прост делител на N. За произволно число a неделящо се на p е в сила $a^{p-1} \equiv 1 \pmod{p}$. Но тогава и за всяка P кратно на $p-1$ е в сила

$$a^P \equiv 1 \pmod{p} \qquad \Longrightarrow \qquad p \mid \gcd(a^P - 1, N).$$

(достатъчно е дори P да се дели на реда на a по модул p.)

Да предположим, че всички прости делители на $p-1$ не надминават някакво число B, т.е. $p-1$ е B-гладко. Тогава да вземем произволно a (разбира се $(a,N) = 1$. ако не то сме намерили делител). Почваме да изчисляваме P, което е произведение само на прости ненадминаващи B и периодично проверяваме дали

$$\gcd(a^P - 1, N) \neq 1.$$

Пример 9.3.1 Нека $N = 13\,843$ и да изберем база от прости числа $\{2,3,5\}$. Нека вземем $a = 2$ и $P = 2^2.3^3$. Изчисленията показват, че

$$\gcd(2^P - 1, N) = 109 \qquad \Longrightarrow \qquad 13\,843 = 109.127$$

Важно! Независимо, че реализацията на алгоритмите за разлагане (поне за големи N) не може да мине без подпрограма за пресмятане с големи цели числа, то операции като 2^P трябва да се извършват по модул (в случая по модул N). Така в изчисленията не се надхвърля значително N.

9.3.2 Метод Pollard rho

Нека p е прост делител на N. Алгоритъмът се базира на факта, че в редица от остатъци по модул N с дължина по-голяма от p трябва да има два остатъка сравними по модул p. Тогава най-големият делител на разликата им и N ще даде делител на N. Алгоритъмът е следния:

Избира се неразложим полином $f(x) \in \mathbb{Z}[x]$, начална стойност x_1 и се конструира итеративно редицата $\{x_i\}_{i=1}^{n}$ чрез

$$x_i = f(x_{i-1}).$$

От дадено място нататък редицата трябва да стане периодична по модул p, т.е. $x_j \equiv x_i \pmod{p}$. Тогава

$$\gcd(x_j - x_i, N)$$

ще даде делител на N. Колко ще бъде периодът на редицата и предпериодичната част ("опашката" на буквата ρ - оттук идва и името на метода) зависи от $f(x)$, x_1 и p, което не е известно. В редица с дължина $\approx \sqrt{N}$ би трябвало да се съдържа поне един период (в действителност периодът може да бъде много по-малък от p).

Пример 9.3.2 Нека $N = 13\,843$ и да изберем $f(x) = x^2 + x + 1$ и $x_1 = 2$. Първите 20 итерации ни дават редицата: $2, 7, 57, 3307, 3587, 10010, 634, 1144, 8639, 13348, 9200, 13099, 12916, 137, 5064, 11925, 8412, 4741, 791, 3538$

Най-големиат общ делител на разликата между осмия и тринадесетия член с N дава

$$\gcd(1144 - 12916, 13843) = 109$$

Периодът на тази редица по модул 109 е 5, а предпериодичната част е с дължина 7.

9.4 Метод Number Field Sieve (NFS)

Този метод е "наследник" (базира се на същата идея) на метода на квадратичното решето. За разлика от него и другите разгледани горе методи сложността му (времето за изпълнение) не зависи от големината на простите делители, а само от N. Затова той се прилага за числа имаше малко, но големи прости делители. Времето за изпълнение се оценява на

$$exp((c+o(1))\sqrt[3]{\ln N(\ln\ln N)^2}),$$

където $c \approx 1.526$ или ≈ 1.923 взависимост от варианта, който се прилага.

Детаилно описание на NFS алгоритъма изисква знания от алгебрична теория на числата, но ще се опитаме да дадем кратко описание на алгоритъма без да надхвърляме знанията полечени от университетския курс по висша алгебра.

Намираме неразложим над $\mathbb{Q}$ полином $f(x) \in \mathbb{Z}[x]$ и $m \in \mathbb{Z}$, такива че

$$f(m) \equiv 0 \pmod{N}, \qquad \text{т.е.} \qquad f(m) = kN.$$

Нека α е корен на $f(x)$ в подходящо разширение на $\mathbb{Q}$ и да разгледаме простото разширение $\mathbb{Q}(\alpha)$. Пръстенът $\mathbb{Z}[\alpha] \subset \mathbb{Q}(\alpha)$ е подпръстен на пръстена на целите алгебрични числа, т.е. на тези елементи на $\mathbb{Q}(\alpha)$, които са корени на полиноми с цели коефициенти.

Намираме множество $S = \{(a,b) \mid a \in [-A, A],\ b \in [1, B],\ \gcd(a,b) = 1\}$ състоящо се от двойки цели числа, такива че

$$b^{\deg(f)} f(\frac{a}{b}) = \|a - b\alpha\|$$

е $\mathcal{B}$-гладко, т.е. дели се само на прости числа ненадминаващи $\mathcal{B}$. Горното число $\|a - b\alpha\|$ е нормата на елемента $a - b\alpha$.

Намираме подмножество $T \subset S$, такова че съществува $\gamma \in \mathbb{Z}[\alpha]$, за което

$$\gamma^2 = \prod_{(a,b)\in T} (a - b\alpha).$$

Тази част е най-трудната в алгоритъма. Реализира се чрез разлагане на $a - b\alpha$ на произведение от прости идеали и използване на подхода описана в началото на главата. По-подробно разглеждане на проблема излиза извън рамките на този курс

Изображението $\varphi;\quad \mathbb{Z}[\alpha] \to \mathbb{Z}_N$ зададено с $\varphi(\alpha) \equiv m \pmod{N}$ е хомомморфизъм и

$$y^2 = \varphi(\gamma)^2 \equiv \prod_{(a,b)\in T} (a - bm) = x^2 \pmod{N}.$$

Надяваме се $y = \varphi(\gamma)$ да е различно от x. Множител на N намираме като $\gcd(N, x \pm y)$.