Talkroppssållet

Lina Mårtensson

$$N = pq$$

- Talkroppssållet snabbast för att faktorisera stora heltal
- RSA Factoring Challenge
- 200-siffrigt tal faktoriserat

Fermats metod

$$N = u^2 - v^2 = (u+v)(u-v)$$

$$N = 8051$$
$$8051 - 90^2 = 49 = 7^2$$
$$8051 = 97 \cdot 83$$

Det kvadratiska sållet

$$u^2 \equiv v^2 \bmod N$$
$$x_i = \lceil \sqrt{N} \rceil + i,\ i = 0, 1, 2 \ldots$$
$$x_i^2 - N = y_i$$

Det kvadratiska sållet

$$46^2 - 2041 = 75$$
$$47^2 - 2041 = 168$$
$$48^2 - 2041 = 263$$
$$49^2 - 2041 = 360$$
$$50^2 - 2041 = 459$$
$$51^2 - 2041 = 560$$

Det kvadratiska sållet

$$75 = 3 \cdot 5^2$$

$$168 = 2^3 \cdot 3 \cdot 7$$

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$560 = 2^4 \cdot 5 \cdot 7$$

Faktorbas

Istället för att faktorisera alla y_i, så bryr vi oss bara om de som har faktorer som är mindre än något tal B. Primtalen som är mindre än B bildar en $faktorbas$. Vi kan även ha med y_i som endast har några få faktorer som är större än B, dock inte större än L.

Det kvadratiska sållet

$$75 \cdot 168 \cdot 360 \cdot 560 = 2^{10} \cdot 3^4 \cdot 5^4 \cdot 7^2$$

$$u = 46 \cdot 47 \cdot 49 \cdot 51 \equiv 311 \bmod 2041$$

$$v = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \equiv 1416 \bmod 2041$$

$$\gcd(1416 - 311, 2041) = 13$$

$$2041 = 13 \cdot 157$$

Det kvadratiska sållet

$$
\begin{array}{cc}
 & \begin{array}{cccc} 2 & 3 & 5 & 7 \end{array} \\
\begin{array}{c} 75 \\ 168 \\ 360 \\ 560 \end{array} & \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}
\end{array}
$$

Grupper

$$\langle G, * \rangle$$

- Sluten under $*$ ($a * b \in G$, $\forall a, b \in G$)
- Associativitet ($(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$)
- Identitet ($\exists e \in G$ sådan att $e * a = a * e = a$, $\forall a \in G$)
- Invers ($\forall a \in G$, $\exists a' \in G$ sådan att $a * a' = a' * a = e$)

Ringar

$$\langle R, +, \cdot \rangle$$

- $\langle R, + \rangle$ är en kommutativ grupp ($a + b = b + a, \ \forall a, b \in R$)
- $\cdot$ är associativ
- Distributiva lagar gäller ($a \cdot (b + c) = ab + ac$, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$, $\forall a, b, c \in R$)

Ringar

- En *delring* av en ring $\langle R, +, \cdot \rangle$ är en delmängd av R som är en ring m.a.p. $+$ och $\cdot$

- En *kommutativ ring* är en ring i vilken den multiplikativa operationen är kommutativ ($a \cdot b = b \cdot a, \forall a, b \in R$)

Kroppar

En kropp K är en kommutativ ring där K är en grupp m.a.p. $+$, och $K \setminus 0$ är en grupp m.a.p. $\cdot$.

Homomorfier

En homomorfi är en mappning från en algebraisk struktur till en annan sådan att deras operationer bevaras.

$$\langle A, * \rangle,\ \langle B, \# \rangle$$
$$\phi : A \to B$$
$$\phi(x * y) = \phi(x) \# \phi(y),\ \forall x, y \in A$$

Ideal

En delring I av en ring R är ett ideal om $ir \in I, \forall i \in I, \forall r \in R$.

$Prima\ ideal$ är ideal sådana att om $ab \in I$ så måste antingen $a \in I$ eller $b \in I$.

Normer

- Normen är ett storleksmått
- Normen av ett primideal är ett rationellt primtal.
- Normen är multiplikativ, dvs $N(ab) = N(a)N(b)$.

Tidskomplexitet för talkroppssållet

$$O\left\{e^{\left(\frac{64}{9}\log N\right)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}\right\}$$

Polynom

$$f_1(m) \equiv 0 \bmod N$$

$$f_2(m) \equiv 0 \bmod N$$

$$f_1(\alpha_1) = 0, f_2(\alpha_2) = 0$$

$$\alpha_1, \alpha_2 \in \mathbb{C}$$

Homomorfier

$$\varphi_1 : \mathbb{Z}[\alpha_1] \longrightarrow \mathbb{Z}_N$$

$$\varphi_2 : \mathbb{Z}[\alpha_2] \longrightarrow \mathbb{Z}_N$$

$$\alpha_1 \mapsto m \bmod N$$

$$\alpha_2 \mapsto m \bmod N$$

$$\varphi_1(\beta_1^2) = \prod_{(a,b)\in S} \varphi_1(a - b\alpha_1) = \prod_{(a,b)\in S} (a - bm) \bmod N$$

$$\varphi_2(\beta_2^2) = \prod_{(a,b)\in S} \varphi_2(a - b\alpha_2) = \prod_{(a,b)\in S} (a - bm) \bmod N$$

$$\varphi_1(\beta_1)^2 \equiv \varphi_2(\beta_2)^2 \bmod N$$

$$\gcd(\varphi_1(\beta_1) \pm \varphi_2(\beta_2), N)$$

$$\beta_1 \in \mathbb{Z}[\alpha_1], \beta_2 \in \mathbb{Z}[\alpha_2]$$

Norm

$$N(a - b\alpha_i) = b^{d_i} f_i(a/b)$$

$$d_i = \deg(f_i)$$

$$N(a - b\alpha_i) = \prod_j p_j^{e_j}$$

$$
\begin{array}{cc}
 & \begin{array}{ccccc}
\overbrace{P_{11} \quad P_{12}}^{p_1} & \overbrace{P_{21} \quad P_{22}}^{p_2} & \overbrace{P_{31} \quad P_{32} \quad P_{33}}^{p_3} & \cdots & \overbrace{P_{km}}^{p_k}
\end{array} \\
\begin{array}{c}
(a_1, b_1) \\
(a_2, b_2) \\
(a_3, b_3) \\
\vdots \\
(a_n, b_n)
\end{array}
&
\begin{bmatrix}
0 & 1 & 0 & 1 & 0 & 2 & 0 & & 0 \\
3 & 0 & 0 & 2 & 0 & 0 & 0 & \cdots & 2 \\
1 & 0 & 2 & 0 & 1 & 0 & 0 & & 0 \\
 & & & \vdots & & & & \ddots & \vdots \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & \cdots & 0
\end{bmatrix}
\end{array}
$$

RSA-640

- Polynomgenerering, troligen CPU-veckor
- $166 \cdot 10^7$ relationer hittades under tre månaders sållning på 80 2.2 GHz Opteron-maskiner
- Faktorbaser: $28 \cdot 10^7$ resp. $15 \cdot 10^7$, övre gräns 2^{34}.
- En matris med $36 \cdot 10^6$ rader och kolumner skapades
- Matrissteget tog 1.5 månad på 80 2.2 GHz Opteron-maskiner