Quadratic Sieve

Avancerade algoritmer (2D1440)
8/11-2000

Joel Brynielsson, TCS/Nada (f.d. D95)

http://www.nada.kth.se/~joel/qs.pdf

Huvudidé

Vill hitta x och y så att

$$x^2 \equiv y^2 \bmod n \qquad x \not\equiv \pm y \bmod n$$

Då vet vi att

$$n|(x^2 - y^2) \iff n|(x + y)(x - y)$$

Vi vet också att n varken delar $(x + y)$ eller $(x - y)$ och således kommer $\gcd(n, x + y)$ och $\gcd(n, x - y)$ vara faktorer till n.

Quadratic Sieve i korthet

Metoden använder en *faktorbas* som är en mängd bestående av ”små” primtal.

Skapa ett antal x_i så att x_i^2 mod n går att faktorisera i faktorbasen.

Vi har nu ett antal samband av typen

$$x_i^2 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

Kombinera några av dessa samband (multiplicera ihop dem) så att båda sidor blir en kvadrat.

Triviala lösningar

Notera att vi har 50% sannolikhet att få triviala lösningar och att vi därför kan behöva köra vår algoritm flera gånger.

Exempel

$n = 15770708441$
Faktorbas: $\{2, 3, 5, 7, 11, 13\}$

Betrakta följande samband:

$$\begin{aligned} 8340934156^2 &\equiv 3 \times 7 \pmod{n} \\ 12044942944^2 &\equiv 2 \times 7 \times 13 \pmod{n} \\ 2773700011^2 &\equiv 2 \times 3 \times 13 \pmod{n} \end{aligned}$$

Tre exponentvektorer:

$$\begin{aligned} a_1 &= (0, 1, 0, 1, 0, 0) \\ a_2 &= (1, 0, 0, 1, 0, 1) \\ a_3 &= (1, 1, 0, 0, 0, 1) \end{aligned}$$

$a_1 + a_2 + a_3 = (0, 0, 0, 0, 0, 0)$ mod 2 så vi får:

$$(8340934156 \times 12044942944 \times 2773700011)^2 \equiv$$

$$\equiv (2 \times 3 \times 7 \times 13)^2 \pmod{n} \iff$$

$$\iff 9503435785^2 \equiv 546^2 \pmod{n}$$

$$\gcd(n, 9503435785 - 546) = 115759$$

115759 är således en faktor i n.

Pomerances idé

Vi använder oss av följande polynom:

$$f(x) = (x + \lfloor\sqrt{n}\rfloor)^2 - n$$

Vi ser att

$$(x + \lfloor\sqrt{n}\rfloor)^2 \equiv f(x) \bmod n$$

Antag nu att vi kan hitta heltal $x_1, x_2, \ldots, x_k$ så att produkten $f(x_1)f(x_2)\ldots f(x_k)$ bildar en kvadrat, y^2. Om vi sedan låter

$$x = (x_1 + \lfloor\sqrt{n}\rfloor)(x_2 + \lfloor\sqrt{n}\rfloor)\ldots(x_k + \lfloor\sqrt{n}\rfloor)$$

har vi en lösning till vår huvudekvation, $x^2 \equiv y^2 \bmod n$.

Att finna faktorbasen

Vi vill välja de primtal, p_i, som ingår i faktorbasen.

Vill ha: $p_i \mid f(x)$

Vet:

$$p_i \nmid n \qquad f(x) = (\lfloor \sqrt{n} \rfloor + x)^2 - n$$

Detta ger oss

$$n \equiv (\lfloor \sqrt{n} \rfloor + x)^2 \bmod p_i$$

Vår faktorbas skall alltså bestå enbart av primtal, p_i, sådana att n är en kvadratisk rest modulo p_i.

Såll 1

Tal som faktoriserar över faktorbasen kommer att vara mycket få.

Ett *såll* ger oss möjlighet att betrakta en mängd värden i ett stort block på en gång och bestämma vilka tal som kommer att kunna faktoriseras.

Såll 2

$$f(x) = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

$$\Updownarrow$$

$$\log f(x) = \log p_1^{a_1} + \log p_2^{a_2} + \ldots + \log p_k^{a_k}$$

Om vi subtraherar bort logaritmen för de p_i som ingår i $f(x)$ från $\log f(x)$ kommer vi teoretiskt sett komma ner till noll om $f(x)$ kan faktoriseras i faktorbasen.

Avrundningsfel och multipla primtal gör att vi i praktiken använder oss av ett gränsvärde så att vi betraktar alla tal som är ”tillräckligt nära”. Gränsvärdet sätts ofta till logaritmen för det största primtalet i faktorbasen.

Såll 3

Hur vet vi om ett primtal ingår i $f(x)$?

Vet att n är kvadratisk rest modulo p, d.v.s.

$$n \equiv t^2 \text{ mod } p \text{ eller } n \equiv (-t)^2 \text{ mod } p$$

För alla p löser vi dessa kongruenser och sparar undan t och $-t$.

Eftersom $n \equiv (\lfloor\sqrt{n}\rfloor + x)^2$ mod p (p.g.a. att $p|f(x)$) betyder detta också att

$\lfloor\sqrt{n}\rfloor + x \equiv t$ mod p eller $\lfloor\sqrt{n}\rfloor + x \equiv -t$ mod p

Om ovanstående är uppfyllt skall vi alltså subtrahera $\log p$ från $\log f(x)$.

Såll 4

Startvärde på x ges av t.

Om p delar $f(x)$ kommer även p att dela $f(x+p), f(x+2p)$ o.s.v.

Detta ger oss basen för vårt såll där vi på detta sätt kan subtrahera bort $\log p$ från en stor mängd $\log f(x)$ utan att behöva göra nya jämförelser.

Lite parametrar

Storlek på faktorbas:
$L(n)^{1/2}$ där $L(n) = O\left(e^{c\sqrt{\ln n \ln \ln n}}\right)$ är körtiden

Antal $f(x)$ att hitta:
faktorbasens storlek + 10

Gränsvärde för sållet:
logaritmen för det största talet i faktorbasen

För varje primtal p i faktorbasen lagras även
$\log p$, t och $-t$.

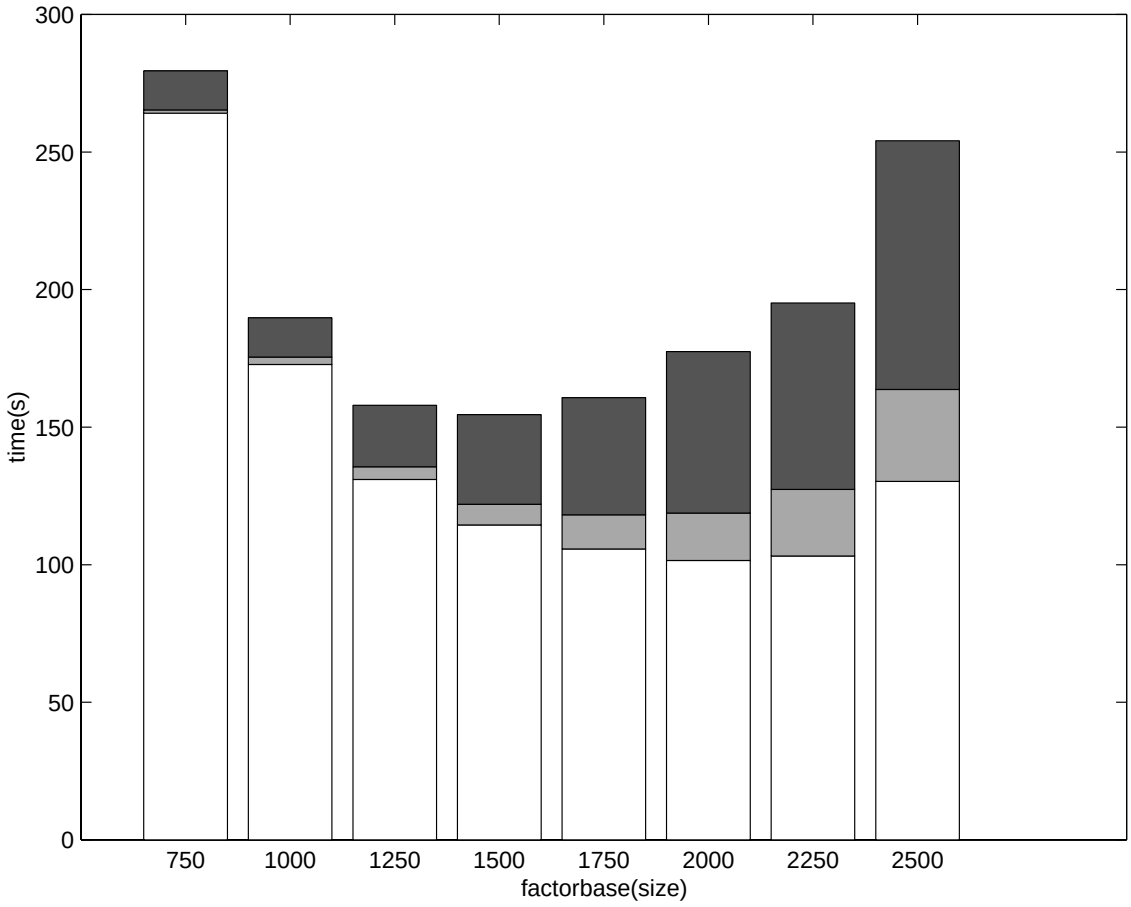
Sållning i två dimensioner

$$f(x) = (x + \lfloor \sqrt{n} \rfloor)^2 - n$$

$$\Downarrow$$

$$f(a, b) = (\lfloor \sqrt{bn} \rfloor + a)^2 - bn$$

Körningar med olika storlekar på faktorbasen för 40-decimalers tal

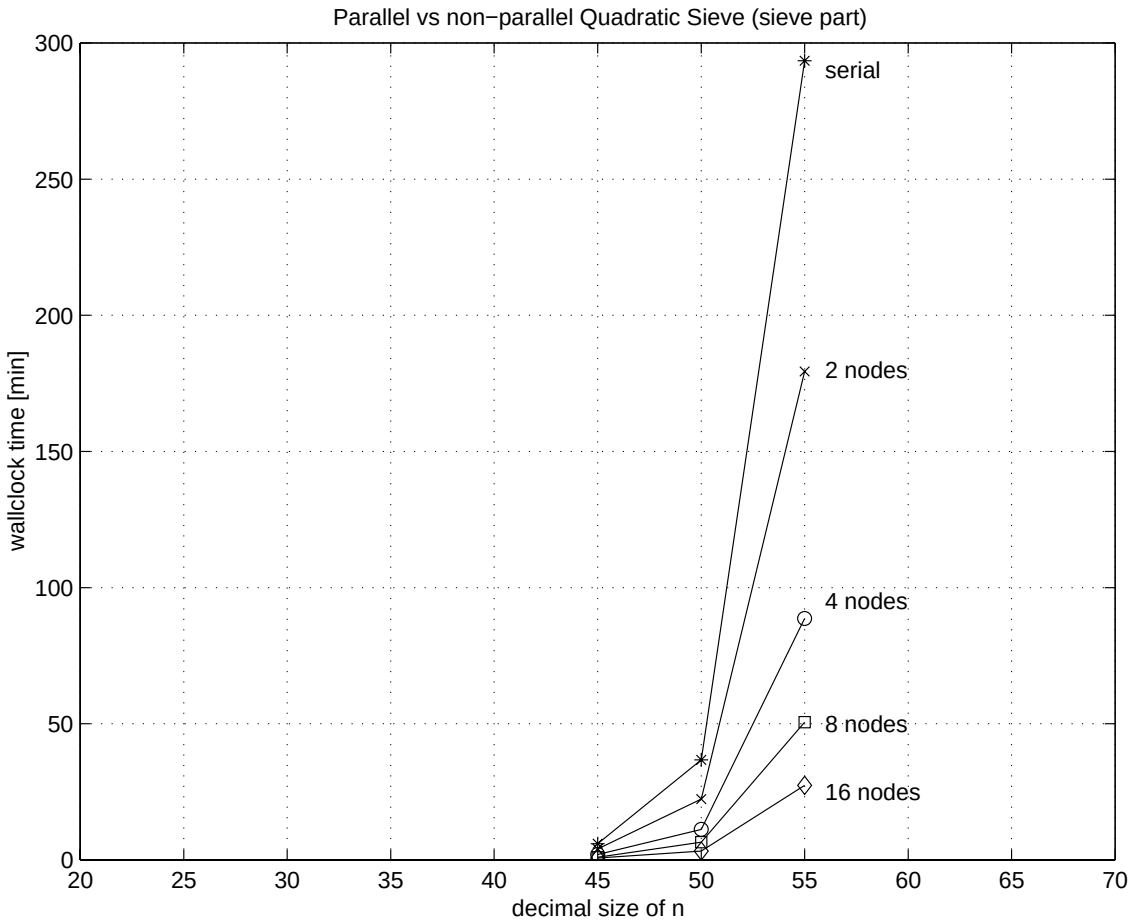


Vit: Såll

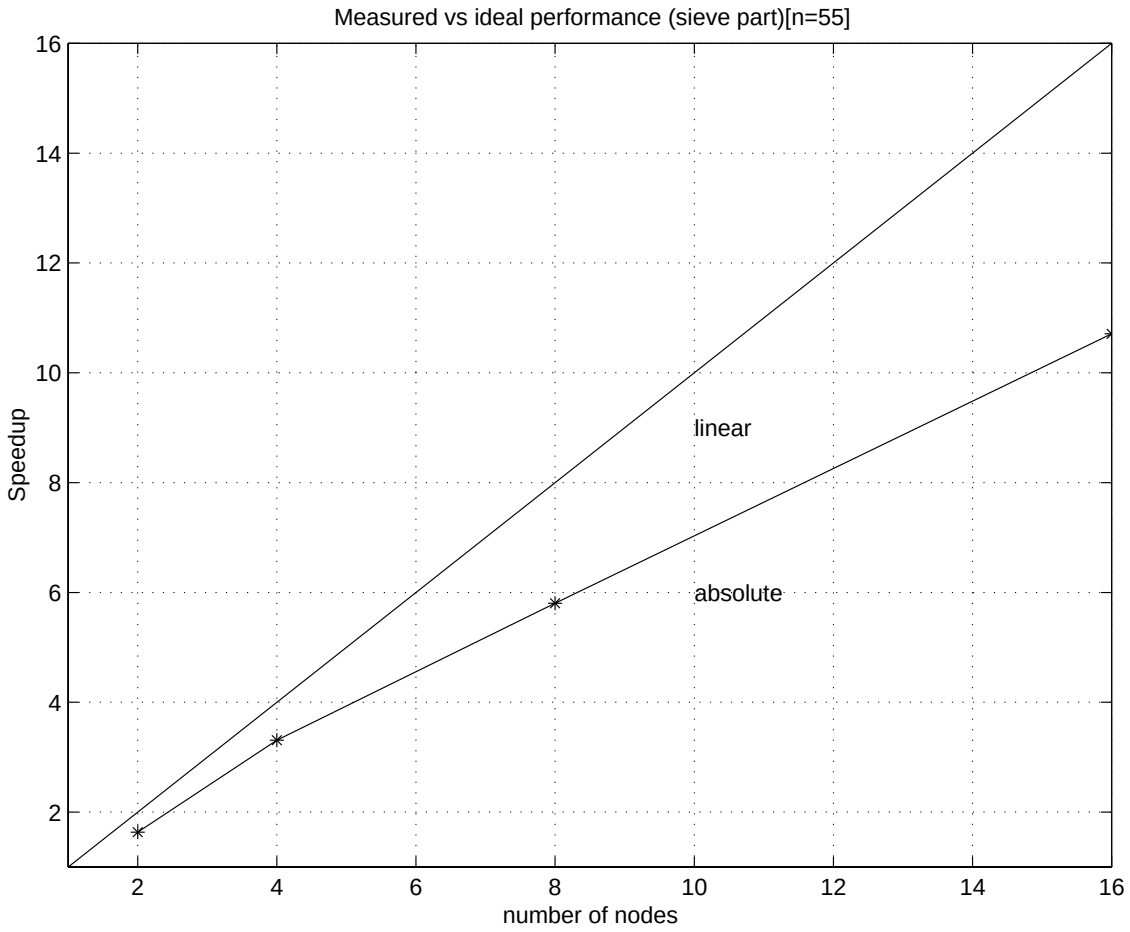
Mörkgrå: Gausselimination

Ljusgrå: Övrigt

Parallell körning 1



Parallell körning 2



Talet som faktoriserats har 50 decimaler.