Subexponentielle Attacken auf RSA und DSA

RSA: Grundidee ist die 3. binomische Formel

$$x^2 - y^2 = (x+y)\cdot(x-y)$$

$225 - 4 = 221 = (15+2)\cdot(15-2) = 17\cdot 13$

$15^2 - 2^2$

↝ Dixon's random square method (1. Version)

$x^2 \bmod n$ erzeugen

bis man ein $y^2 \bmod n$ erhält

Beispiel: $n = 209$

$x = 24$, $x^2 \equiv 158 \bmod 209$

$x = 25$, $x^2 \equiv 207 \bmod 209$

$x = 26$, $x^2 \equiv 49 \bmod 209$

zufällige x-Werte

$26^2 \equiv 7^2 \bmod 209$

$26^2 - 7^2 \equiv 0 \bmod 209$

$209 \mid 26^2 - 7^2$ $\quad (209 \mid 627)$

$209 \mid (26-7)\cdot(26+7)$

ggT 19 · 33 ggT

$ggT(209,19) = 19$

$ggT(209,33) = 11$

Quadrate per Zufall erzeugen ist nicht sehr wahrscheinlich ⇝ weiterer Trick nötig

⇝ 2. Version

nutze Fehlschläge ebenfalls aus, um Quadrate zu erzeugen

Beispiel: $n = 165$

$x = 20$: $x^2 \equiv 70 \equiv 2 \cdot 5 \cdot 7 \mod 165$

$x = 21$: $x^2 \equiv 111 \equiv 3 \cdot 37 \mod 165$

$x = 22$: $x^2 \equiv 154 \equiv 2 \cdot 7 \cdot 11 \mod 165$

$x = 23$: 34

$x = 24$ x^2 81 3^2 mod 165 (1. Version)

$x = 25$ 130

$x = 26$ 16

$x = 27$ 69

$x = 28$ 124

$x = 29$ 16

$x = 30$ $75 \equiv 3 \cdot 5^2 \mod 165$

$x = 31$ 136

$x = 32$ 34

$x = 33$ 99

$x = 34$ 1

$x = 35$ siehe oben

$x = 20$

$35^2 \equiv 70 \equiv 2 \cdot 5 \cdot 7 \mod 165$

$20^2 \equiv 70 \equiv 2 \cdot 5 \cdot 7 \mod 165$

$(\underbrace{35 \cdot 20}_{x = 700})^2 \equiv 35^2 \cdot 20^2 \equiv 2^2 \cdot 5^2 \cdot 7^2 \mod 165$

$\equiv (\underbrace{2 \cdot 5 \cdot 7}_{y = 70})^2$

$\Rightarrow ggT(165, x - y)$

$= ggT(165, 630) = 15$, $ggT(165, x + y)$

$ggT(165, 770) = 55$

$165 = 15 \cdot 11 = 3 \cdot 5 \cdot 11$

Zusammenfassung:

- Quadrieren von zufälligen x-Werten mod n
- Zerlege x^2 mod n in kleine Primfaktoren [Obergrenze]
- Kombiniere erfolgreiche Zerlegungen zu y^2

$$x_1^2 \cdot x_2^2 \cdot x_3^2 \cdots \equiv y^2 \bmod n$$

- $ggT(x-y, n)$, $ggT(x+y, n)$ sind wahrscheinlich echte Faktoren von n

Laufzeit abhängig von der Wahrscheinlichkeit, mit der zufällige y in Primzahlen ≤ Obergrenze zerlegt werden können.

Laufzeiten haben die Form

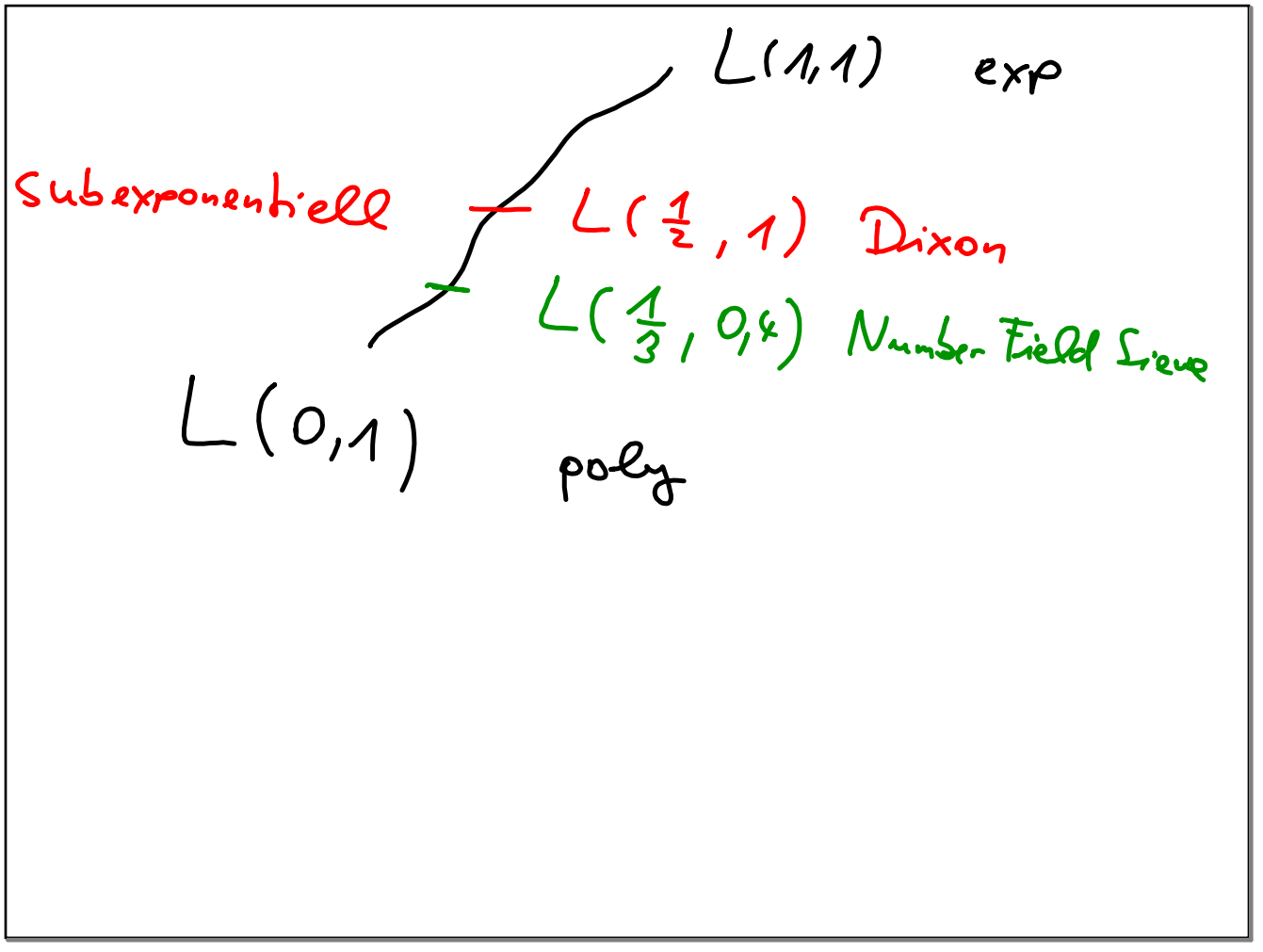
$$L_n(\varepsilon, \delta) = \exp\left(\delta \cdot \log_n^{\varepsilon} \cdot (\log\log n)^{1-\varepsilon}\right)$$

setze $\delta = 1$, $\varepsilon = 1$: $L(1,1) = \exp(\log_n^1) = n$

setze $\delta = 1$, $\varepsilon = 0$: $L(0,1) = \exp(\log \log_n n) = \log n$

☐ $L(1,1)$ exponentiell

☐ $L(0,1)$ polynomiell


L(1,1) exp
subexponentiell
L(1/2, 1) Dixon
L(1/3, 0,4) Number Field Sieve
L(0,1) poly