

# Outline: Discrete Logarithm Problem

Jonathan Lee

July 10, 2002

## 1 Preliminaries

- definitions: suppose  $G = \langle \gamma \rangle$ 
  - order of  $\alpha \in G$ :  $\min \{x \in \mathbb{Z}^+ : \gamma^x = \alpha\}$
  - exponent of  $G$ :  $\min \{x \in \mathbb{Z}^+ : g^x = 1 \forall g \in G\} = \text{lcm} \{\text{ord}_g 1 : g \in G\}$
- generalized discrete logarithm problem for infinite cyclic groups generally applies in non-cryptographic contexts (harder for curves)

## 2 Silver-Pohlig-Hellman method

- reduces problem to subproblems in group's prime decomposition ( $(n, m) = 1 \iff C_{nm} = C_n \times C_m$ )
  - subproblem: finding  $\text{ord}_{\gamma_p} \alpha_p$ , where  $\gamma_p = \gamma^{n/p^{e_p}}$ ,  $\alpha_p = \alpha^{n/p^{e_p}}$  (notice:  $\text{ord}_{\gamma} \gamma_p = p^{e_p}$ )
  - determine  $x$ ,  $x \equiv \text{ord}_{\gamma_p} \alpha_p \pmod{p^{e_p}}$  for all  $p$  (note that for all  $p$ :  $1 = \gamma_p^{-x_p} \alpha_p = (\gamma^{-x_p} \alpha)^{n/p^{e_p}} = (\gamma^{-x_p + k \cdot p^{e_p}} \alpha)^{n/p^{e_p}} = (\gamma^{-x} \alpha)^{n/p^{e_p}}$ )
- further reduction from prime-power-order groups to prime-order groups
  - suppose  $|G| = p^e$ , and let  $\sum_{i=0}^{e-1} x_i p^i$  be the base- $p$  expansion of  $\text{ord}_{\gamma} x$
  - defining  $a_i = \alpha \cdot \gamma^{-\sum_{n=0}^i x_n p^n}$ , we obtain  $(\gamma^{p^{e-1}})^{x_i} = a_i^{p^{e-i-1}}$ ,  $0 \leq i \leq e-1$
- actual algorithm - reduce to prime-power case (Chinese Remainder Theorem), reduce to prime case (Lagrange's Theorem / Fermat's Little Theorem), solve (Baby-Step, Giant Step /  $\rho$ -algorithm)
  - runtime:  $O\left(\sum_{p||G|} (e_p (\log |G| + \sqrt{p}))\right)$
  - works best with small prime factors (Mersenne primes advantageous)

## 3 Index Calculus Method

- more suited to prime-powered groups, ie.  $\mathbb{F}_{p^n}$
- re-introduction of factor bases
  - note that if  $\alpha = \prod_i \alpha_i$ , then  $\text{ord}_{\gamma} \alpha \equiv \sum_i \text{ord}_{\gamma} \alpha_i \pmod{|G|}$
  - compute  $\text{ord}_{\gamma} v$  for  $v$  in factor base
    - \* take exponent vectors for  $\{\alpha^t\}$ , note that  $t \equiv \sum_i \text{ord}_{\gamma} \alpha_i^{e_i} \pmod{|\langle \gamma \rangle|}$
    - \* acquire independent set of  $|\{v\}|$  relations, solve to obtain  $\text{ord}_{\gamma} v$
- determine  $\text{ord}_{\gamma} \alpha$

- find  $t$  so that  $\alpha\gamma^t$  is smooth
- factor and obtain  $\text{ord}_\alpha \equiv \sum_i \text{ord}_\gamma(\alpha\gamma)_i \cdot e_i - t \pmod{|\langle \gamma \rangle|}$