How to determine the mult. order of an element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$?

<u>Thm 15.10</u> (Baby-step giant-step alg.)

Assume we can perform arithmetic in the group $G$ in $O(1)$ and we can compare elements w.r.t. some total order on $G$ in $O(1)$. We can compute the order $k < \infty$ of a (torsion) element $a \in G$ in time $O(\sqrt{k} \log k)$ with memory $O(\sqrt{k})$.

<u>Idea</u> Let $w > \sqrt{k}$.

Write $k = iw + j$ with $1 \leq j \leq w$, $0 \leq i \leq w-1$.

$$a^k = 1 \iff \underbrace{a^{iw}}_{=(a^w)^i} = a^{-j}$$

$(a^w)^i$: giant step

$a^{-j}$: baby step

<u>Alg</u> For $e = 1, 2, \ldots$:

Let $w = 2^e$.

Compute $a^{-j}$ for $j = 1, \ldots, w$ and save the pairs $(a^{-j}, j)$ in a binary search tree (BST).

For $i = 0, 1, \ldots, w-1$:

Compute $(a^w)^i$. If there exists some $j$ in the BST with $a^{-j} = (a^w)^i$, return the smallest such $iw+j$.

<u>Rmk</u> Better to use a hashtable...

<u>Rmk</u> Combining this with Lemma 15.9, we can find a nontriv. factor of a composite integer $n$ in $O(\sqrt{n})$.

"Yay..."

<u>Problem</u> 1) BSGS alg. too slow. There are better algorithms for the group $(\mathbb{Z}/n\mathbb{Z})^\times$ (e.g. the <u>index calculus algorithm</u>).

2) $(\mathbb{Z}/n\mathbb{Z})^\times$ too large. The class group of $\mathbb{Q}(\sqrt{-n})$ has just order $O(\sqrt{n})$. Its 2-torsion elements "correspond to"

divisors of $n$. (Shanks's class group method).

Rmk On a quantum RAM, we can compute the mult. order of any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ in time polynomial in $\log n$. (Shor's algorithm)

Lemma 15.11 Let $n \geq 2$, let $p$ be a prime dividing $n$ and let $t \geq 1$ such that $p-1 \mid t!$. Then, the following alg. returns a divisor $d \geq 2$ of $n$ in time $\tilde{O}(t \log n)$.

Alg (Pollard's $p-1$ alg.)

Pick $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ at random.

For $k = 1, 2, \ldots$:

Compute $a^{k!} \bmod n$

$$\overset{\shortparallel}{\left(a^{(k-1)!}\right)^k}$$

If $d := \gcd(a^{k!} - 1, n) > 1$, return $d$.

Pf $p-1 \mid k! \Rightarrow \operatorname{ord}(a \bmod p) \mid k! \Rightarrow a^{k!} \equiv 1 \bmod p$
$\Rightarrow p \mid d$. $\square$

Problems 1) The alg. might return the trivial divisor $d = n$.
(If $n = pq$ and ($p-1 \mid t! \Leftrightarrow q-1 \mid t!$), this could happen for many $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.)

2) $t$ could be large:
E.g. if $p - 1 = 2q$ for a prime $q$, then we need $t \geq q$, which could be $\Omega(\sqrt{n})$ even for the smallest prime factor $p$ of $n$.

Rmk We can get rid of the problems by replacing $(\mathbb{Z}/n\mathbb{Z})^\times$ by groups $E(\mathbb{Z}/n\mathbb{Z})$ for elliptic curves $E$. (Lenstra's elliptic curve method)

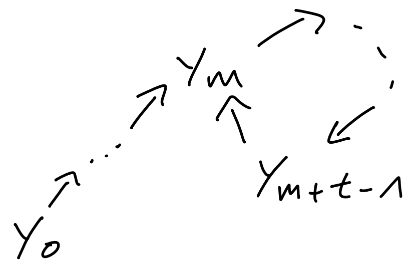
## 15.1. Pollard's rho algorithm (cf. Cohen)

Lemma 15.1.1 Let $f: \{1, \dots, n\} \to \{1, \dots, n\}$ be a uniformly random map. Let $M, T$ be the preperiod and period of the sequence

$$1, f(1), f(f(1)), \dots \qquad (y_i = f^i(1)).$$

We have $\mathbb{E}(M+T) \asymp \sqrt{n}$.

Pf (sketch)




$$\mathbb{P}(M=m, T=t) = \Bigg( \underbrace{\prod_{k=1}^{m+t-1} \left(1 - \frac{k}{n}\right)}_{\mathbb{P}(y_k \neq y_0, \dots, y_{k-1})} \Bigg) \cdot \underbrace{\frac{1}{n}}_{\mathbb{P}(f(y_{m+t-1}) = y_m)}$$

$$\sum_{k=1}^{m+t-1} \log\left(1 - \frac{k}{n}\right) \approx - \sum_k \frac{k}{n} \approx - \frac{(m+t)^2}{2n}$$

$$\Rightarrow \mathbb{P}(M=m, T=t) \approx e^{-(m+t)^2/2n} \cdot \frac{1}{n}.$$

$$\Rightarrow \mathbb{E}(M+T) = \sum_{m,t} \mathbb{P}(M=m, T=t)\cdot(m+t)$$

$$\approx \sum_{m,t} e^{-(m+t)^2/2n} \cdot (m+t) \cdot \frac{1}{n}$$

$$\approx \int_1^\infty \int_1^\infty e^{-(m+t)^2/2n} \cdot (m+t) \cdot \frac{1}{n}\, dm\, dt$$

$$\underset{\substack{m = a\sqrt{n} \\ t = b\sqrt{n}}}{\approx} \underbrace{\int_0^\infty \int_0^\infty e^{-(a+b)^2/2} (a+b)}_{\in (0,\infty)} \cdot \sqrt{n} \cdot da\, db$$

$$\sim \sqrt{n}.$$

"□"

**Thm 15.1.2** Let $n = p_1^{e_1} \cdots p_k^{e_k}$ (with $p_1^{e_1} < \dots < p_k^{e_k}$), $k \geq 2$. Assume $f_1, \dots, f_k$ are (independent) uniformly random functions, $f_i : \mathbb{Z}/p_i^{e_i}\mathbb{Z} \to \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. They give rise to a function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Assuming we can evaluate $f$ in $\mathcal{O}(1)$, the following alg. returns a divisor $1 < d \leq n$ of $n$ in expected time $\mathcal{O}(\sqrt{p_1^{e_1}} \log n)$. With probability $> \varepsilon$, we have $d < n$. (For some constant $\varepsilon > 0$.)

Alg Let $a = f(0 \bmod n)$, $b = f(a)$.

For $j = 1, 2, \dots$:

($Now$, $a = f^{j}(0)$, $b = f^{2j}(0)$.)

If $d = \gcd(a-b, n) > 1$, return $d$.

Let $a \leftarrow f(a)$, $b \leftarrow f^{2}(b)$.

Pf

Let $m_i, t_i$ be the preperiod and period of $0$ for the function $f_i$. We have $p_i^{e_i} \mid f^{j}(0) - f^{2j}(0)$ if and only if $t_i \mid j$ and $j \geq m_i$.

$\Rightarrow$ The number of steps taken by the alg. is at most the smallest multiple of $t_1$ which $\geq m_1$, which is $\leq t_1 + m_1$, which on average is $O(\sqrt{p_1^{e_1}})$.

The prob. that the smallest $j$ s.t. $t_i \mid j$ and $j \geq m_i$ is the same number for all $i$ is $< 1 - \varepsilon$ for some constant $\varepsilon > 0$. $\square$

Rmk We don't know how to generate a random function $f$ as in the Thm.

Instead, usually the following heuristic is used:

Take $f(X) = X^2 + c$ for a random (fixed) number $c \in \mathbb{Z}/n\mathbb{Z}$.