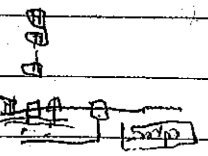
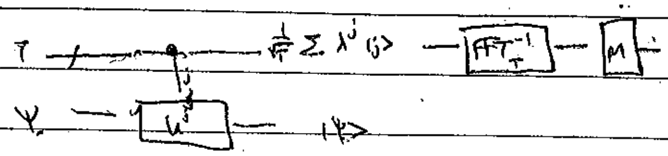
תזכורת



לקוונטים מעל $\mathbb{Z}_2^n$

" " $\mathbb{Z}_{2^n}$

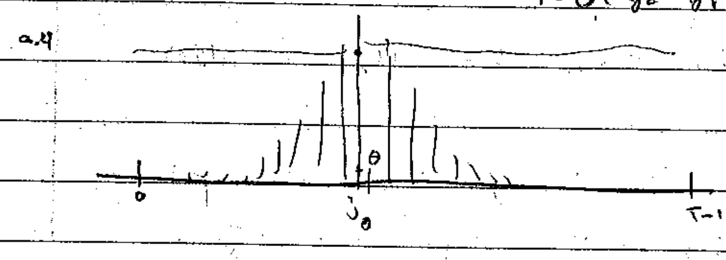
phase estimation



אם $\lambda = \omega^k$ $0 \le k \le T-1$ נקבל את $|k\rangle$ בדיוק.

אם $w = e^{\theta i}$, $T = O(\log\frac{1}{\varepsilon} + \log\frac{1}{\delta})$

לא בהכרח של k



θ קרוב ל $\frac{j_0}{T}$.

טענה: 1. $pr(j_0) \ge 0.4$

2. $pr(j \mid |\frac{j}{T} - \theta| \ge \varepsilon) \le \delta$

<u>קוונטי פורייה מעל $\mathbb{Z}_p$</u> FFT_p^{-1} p ראשוני.

- נקח n ונמצא p ... 2 המשוואה שבלוק ... p

$$2^{n-1} \le p \le 2^n$$

- נגדיר $U: [0..p-1] \to [0..p-1]$

ע"י $U(x) = (x+1) \pmod p$

נשים לב שנרחיב קצת.

$$U(x) = \begin{cases} (x+1) \bmod p & x \in \{0, \dots, p-1\} \\ x & x \in \{p, \dots, 2^n-1\} \end{cases}$$

ונראה [illegible].

U פרמוטציה על הבסיס ולכן אוניטרית.

$$U = \begin{pmatrix} 0 & & 0 & 1 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}$$

על $\mathbb{Z}_p$ U הוא P_p

$$U_{ij} = \begin{cases} 1 & j-i = 1 \\ 0 & \text{אחרת} \end{cases}$$

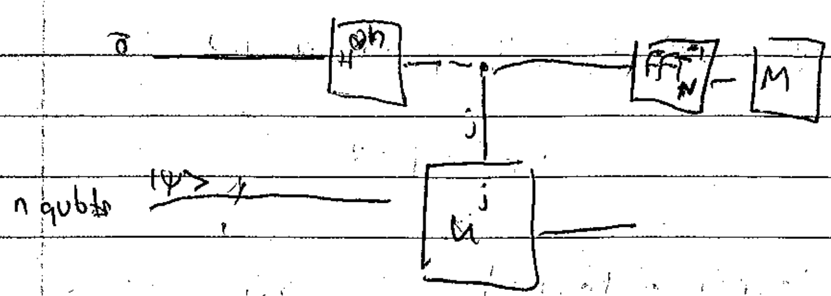
ולכן הו"ע שלה הם הקרקטרים של $\mathbb{Z}_p$ $v_t = \frac{1}{\sqrt{p}} \sum_k \chi_t(k)|k\rangle$

[illegible], $\chi_t(k) = \omega_p^{tk} = e^{-2\pi i \frac{tk}{p}}$

והע"ע של v_t הוא $\lambda_t = \omega^{-t} = e^{-\frac{2\pi i t}{p}}$

שלב 1:

את הנימוקים!



אם $\Psi = |V_t\rangle$ בהסת' $1-\delta$, מקבלים θ קרוב (עד כדי ε) ל- $\frac{t}{p}$: $|\theta-\frac{t}{p}| \le \varepsilon$ כאשר $\varepsilon = \frac{1}{2p}$.

שלב 2 הפונק' j,

נגדיר t_0 השלם הכי קרוב ל- θp.

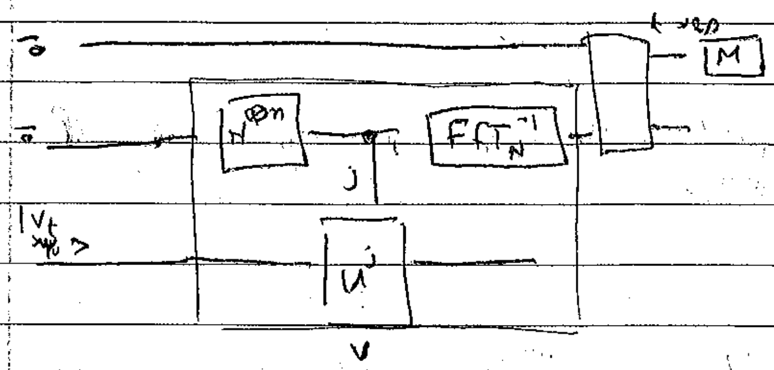
טענה חוץ מהסתברות δ, מתקיים $t_0 = t$.

$$Pr[t_0 = t] \ge Pr\left[|\theta - \tfrac{t}{p}| \le \varepsilon\right] \ge 1-\delta$$

הוכחה נניח $|\theta-\frac{t}{p}| \le \varepsilon$. אז $|\theta p - t| \le \varepsilon p \le \frac{1}{2}$. לכן נקבל תשובה t. □

לכן: חוץ מהסתברות δ אנו נקבל את t

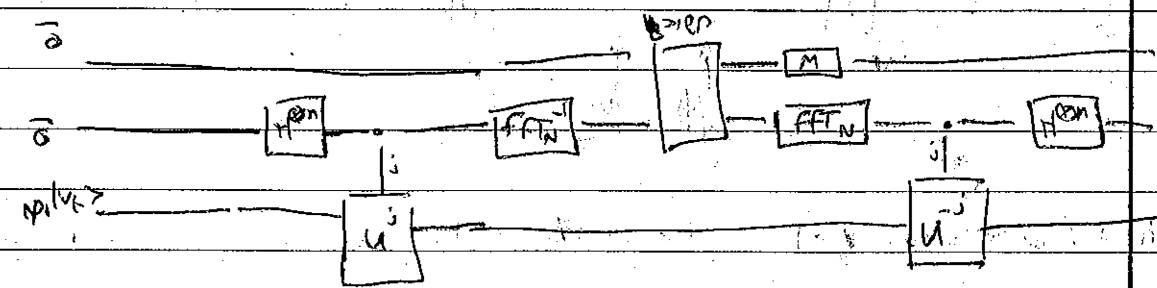
מה שעושה המעגל:
שלב 1:



ונקבל שאנו "לא קרובים" למצב

$$V(|0\rangle \otimes |\Psi\rangle) \otimes |t\rangle$$

עכשיו נפעיל V^{-1}, כלומר, המעגל ההפוך:



ונקבל שאנו "לא (?) קרובים" למצב

$$V^{\dagger} V (|0\rangle \otimes |\Psi_t\rangle) \otimes |t\rangle = |0\rangle \otimes |v_t\rangle \otimes |t\rangle$$

איך מגדירים שמצב אחד קרוב למצב אחר?
יש כמה אפשרויות:
1. בין pure states Ψ_1, Ψ_2
ה fidelity היא $|\langle \Psi_1, \Psi_2 \rangle|$
יש לזה הכללה גם ל mixed states
2. בין mixed states $\| |\Psi_1\rangle\langle\Psi_1| - |\Psi_2\rangle\langle\Psi_2| \|_{tr}$.
נדבר על זה בהמשך.

לא נכון: שנינו אלה מקבלים /שאלה לבדוק:

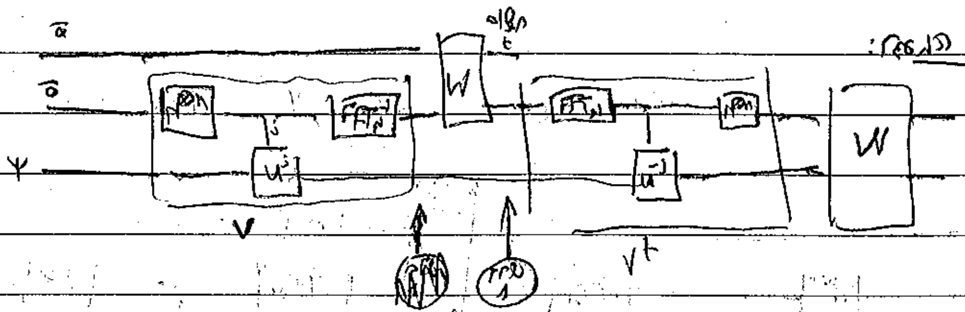
$|V_t\rangle \rightarrow |V_0\rangle \otimes |t\rangle$

סוף: נגדיר לכל $W|k,t\rangle = \omega^{-kt}|k,t\rangle$

אז: $W|\Psi_{k,t}\rangle = W\frac{1}{\sqrt{n}}\sum_{k,t}\omega^{kt}|k,t\rangle$

$= \frac{1}{\sqrt{n}}\sum_{k,t}\omega^{-kt}\omega^{kt}|k,t\rangle = V_0 \otimes |t\rangle$

ובסה"כ הגענו:



מקבל: $A(|0\rangle \otimes |0\rangle \otimes |\Psi_t\rangle) = |t\rangle \otimes |\Psi_0\rangle \otimes |v_0\rangle$

$A(|0\rangle \otimes |0\rangle \otimes \Psi\rangle = FFT_p^{-1}(\Psi) \otimes |0\rangle \otimes |v_0\rangle$

חוץ מזמן הקריאה

המשך ההוכחה:

אם הקלט $|0\rangle\otimes|0\rangle\otimes|v_t\rangle$!

הערה 1: מתקיים (בסיום ה $\widehat{FTP}_p$ המקורי) $\tilde{\varphi} = \sum_j \sum_m \tilde{\alpha}_{j,m} |j,m\rangle \otimes |v_t\rangle$

ולכן ידוע $\sum_{j\neq j_0} \sum_m |\tilde{\alpha}_{j,m}|^2 \leq \delta$

נסמן את המקרה הכללי:

$\tilde{\tilde{\varphi}} = |t\rangle \otimes V(|0\rangle \otimes |v_t\rangle)$

$\tilde{\tilde{\varphi}}$ מתקבל מ $\tilde{\varphi}$ ע"י שינוי הסדר של האיברים במקור W מ $j\neq t$ ל t.

במילים: ~~$\tilde{\alpha}_{j,m} = \tilde{\tilde{\alpha}}_{j,m}$~~ $j\neq t$ אחרת

~~$|\langle\tilde{\varphi},\tilde{\tilde{\varphi}}\rangle| = |\sum_m \bar{\alpha}_{t,m} \tilde{\alpha}_{t,m}| \geq \sum_m |\alpha_{t,m}|^2 \geq 1-\delta$~~

כלומר: אם m ערך מתאים ל t, אז $\alpha_{j,m} = \tilde{\alpha}_{j,m}$

אם m ערך מתאים ל $t' \neq t$ אז מוחלף $\tilde{\alpha}_{t',m}$ עם $\tilde{\tilde{\alpha}}_{t,m}$.

לכן:

$|\langle\varphi,\tilde{\varphi}\rangle| = \sum_{m \text{ מתאים ל } t} |\alpha_{j,m}|^2 \geq 1-\delta$

מכאן שמצבים הם ... ולכן ...

$|\langle \psi_{final}, \tilde{\psi}_{final} \rangle| \geq 1-\delta$. □

תזכורת: אם ψ_1, ψ_2 pure states

$$\frac{1}{2} \left\| |\psi_1\rangle\langle\psi_1| - |\psi_2\rangle\langle\psi_2| \right\|_{tr} = \sqrt{1-|\langle\psi_1|\psi_2\rangle|^2}$$

... adv.

אם $V = \sum_t \alpha_t V_t$

$$\tilde{A}V = \sum_t \alpha_t A V_t = \sum_t \alpha_t \tilde{\varphi}_t$$

$$\tilde{\tilde{A}}V = \sum_t \alpha_t \tilde{\tilde{\varphi}}_t$$

$$|\langle \tilde{A}V, \tilde{\tilde{A}}V \rangle| = \left| \sum_{t_1,t_2} \overline{\alpha_{t_1}} \alpha_{t_2} \langle \tilde{\varphi}_{t_1}, \tilde{\tilde{\varphi}}_{t_2} \rangle \right|$$

$$\geq \left| \sum_t |\alpha_t|^2 \langle \tilde{\varphi}_t, \tilde{\tilde{\varphi}}_t \rangle \right| - \left| \sum_{t_1 \neq t_2} \overline{\alpha_{t_1}} \alpha_{t_2} \langle \tilde{\varphi}_{t_1}, \tilde{\tilde{\varphi}}_{t_2} \rangle \right|$$

$$\geq (1-\delta) \underbrace{\sum_t |\alpha_t|^2}_{=1} - \sum_{t_1 \neq t_2} \alpha_{t_1} \alpha_{t_2} \underbrace{|\langle \tilde{\varphi}_{t_1}, \tilde{\tilde{\varphi}}_{t_2} \rangle|}_{\leq \delta}$$

$t_1 \neq t_2$ ... $\sqrt{\delta}$

$$\leq \sum \sqrt{|\alpha_t|^2} \sqrt{\ldots} = 1$$

$\geq 1 - 2\delta$ ..

תת-חבורה H :1 טענה

1) $(k_1,l_1)\in H$ $\Leftarrow$ $k_1+l_1 s=0$

$(k_2,l_2)\in H$ $\Leftarrow$ $k_2+l_2 s=0$

$\Leftarrow$ $(k_1+k_2)+(l_1+l_2)s=0$

$\Leftarrow$ $(k_1+k_2,\ l_1+l_2)\in H$

2) $(k,l)\in H$ $\Leftarrow$ $k+ls=0$

$\Leftarrow$ $(-k)+(-l)s=0=0$

$\Leftarrow$ $(k,l)^{-1}=(-k,-l)\in H$ $\Leftarrow$

□

טענה 2: $(-s,1)\in H$ אז כל איברי H

הוכחה: יהי $(-s,1)\in H$

אזי

$(k,l)\in H$ יהי

i) $(k,l)=0\cdot(-s,1)$ $\Leftarrow$ $k=0$ $\Leftarrow$ $l=0$

ii) $l\neq 0$ $\Leftarrow$ $(k,l)=l\,(\underbrace{kl^{-1}(p)}_{-s},\ 1)$

$k+ls=0$:מ.ש.ל

$k=-ls$ (p

$\frac{k}{l}=-s$

□

משפט: H תת חבורה של C אז

$C=(c,\omega)+H$

الحل

1) لدينا $(k,\ell) \in H$

$$(c,0)+(k,\ell)=(c+k,\ell)$$

$$c+k+\ell = c+(k+\ell)=c$$

لدن

$$(c,0)+(k,\ell) \in C$$

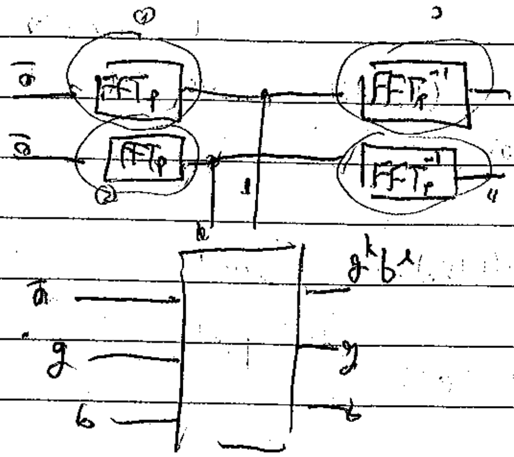
2) لدينا $(k_1,\ell_1) \in C$

ولكن $(k_1-c,\ell_1) \in H$

لدن

$$C \subseteq (c,0)+H$$

⑧ פתרון גם DLOG!



מוגדר $(k,l) \in F_p \times F_p$ אופייני:

כך ש: $\chi_{k,l}|_H = \chi_{k,l}$

כלומר: $\chi_{k,l}(-s,1) = 1$

$$w^{-sk+l} = w^0$$

$$-sk+l = 0$$

$$l = sk$$

אם קיבלנו $k \neq 0$ (קורה בהסת' $1-\frac{1}{p}$)

אז מצאנו $s = \frac{l}{k}$

כמו שראינו FT_{P_p}

Order finding

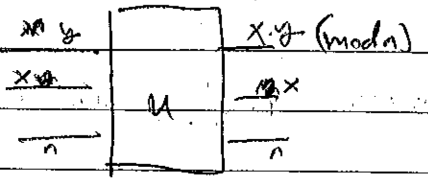
- הגדרה $\mathbb{Z}_n^*$

הבעיה: נתון $x \in \mathbb{Z}_n^*$, n
מצא סדר של n

הסדר: המינימלי כך ש
r מינ' כך $x^j \neq 1$, $\langle x \rangle = x^0, x^1, \dots, x^r = 1$

הפתרון: נגדיר $U = U_x$
שמוגדר על $y \in \mathbb{Z}_n^*$

(אם $y \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ נגדיר U להיות זהות.
זה לא רוצים $y \to xy$.)



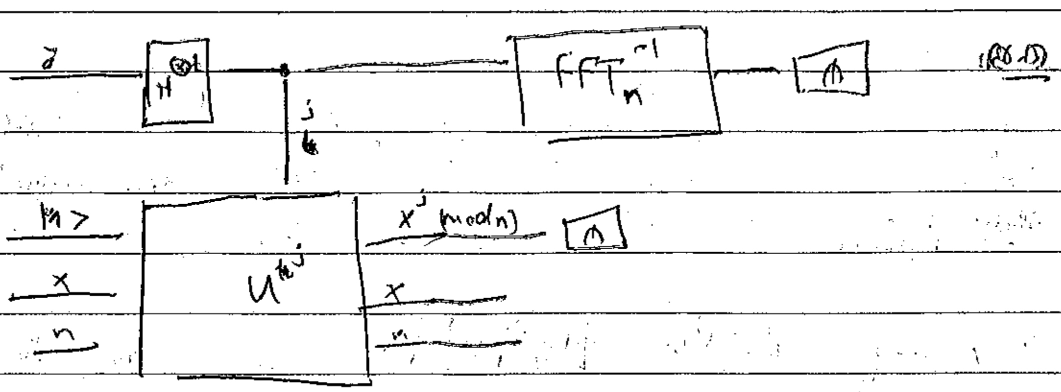
זה מוגדר טוב => הוכיח: U הוא פרמוטציה עלכן יוניטרי
הפיכה

$U: |x, y, n\rangle \to |x, x \cdot y \pmod{n}, n\rangle$

אם $U|x, y_1, n\rangle = U|x, y_2, n\rangle$ אז
$x y_1 = x y_2 \ (n)$

הכפל $x^{-1} (n)$ ⇐ ק"ם ⇐ $x \in \mathbb{Z}_n^*$
ולכן $y_1 = y_2 \ (n)$

U^j — ניתן לחשב ע"י fast exponentiation



למעשה אנו עובדים בבחירת x שנבחר עם x
שהסדר שלו r

הערה: U הוא בעצם הטרנספורמציה $j \to (j+1) \pmod r$

לכן אם היה נכנס לו U, שהוא ו"ע של x_l
הפאזה היתה מקרב את הפאזה $e^{\frac{2\pi i}{r}\cdot l}$
והמעגל היה מוציא קרוב ל $\frac{l}{r}$

ושמנו לב: $\left(\frac{1}{\sqrt r}\sum_{l=1}^{r}\hat x_l\right)(t) = \frac{1}{\sqrt r}\frac{1}{\sqrt r}\sum_{l=1}^{r}\omega^{lt}$

$0 \in k\neq 0$ $x_t - \hat x_t$ מעבירים 1 ל קואורד.

$1 \in k=0$

יוצא $\frac{1}{\sqrt r}\sum_{l=1}^{r}\hat x_l = |1\rangle$

ולכן אפשר לחשוב שאנו מבצעים בבסיס $\hat x_1, \dots, \hat x_r$
ומקבלים כל אחד בהסתברות שווה
ואז מבצעים phase estimation ומקבלים קירוב
בהסתברות $1-\delta$, קרוב ε, של $\frac{l}{r}$

$$pr\left[\,\left|\theta - \frac{l}{r}\right| \le \varepsilon\,\right] \ge 1-\delta$$

M

θ. עשרוני של $\frac{\ell}{r}$, הבאה שלא יהיו יותר מדי r.

למה: יהי $\theta \in [0,1]$, N שלם.
יש לכל היותר שבר יחיד $\frac{a}{b}$ כך ש:

1. $0 \le a,b \le N$, $0<b$, a,b שלמים.
2. $(a,b)=1$ (a זר ל b)
3. $\left|\frac{a}{b}-\theta\right| < \frac{1}{2N^2}$

הוכחה: נניח יש שני שברים כאלה

$$\left|\frac{a_1}{b_1}-\frac{a_2}{b_2}\right| < 2\cdot\frac{1}{2N^2}=\frac{1}{N^2}$$

$$|\underbrace{a_1b_2}_{\text{שלם}}-\underbrace{a_2b_1}_{\text{שלם}}| < \frac{1}{N^2}\cdot b_1b_2 \le \frac{N^2}{N^2} \le 1$$

לכן $a_1b_2=a_2b_1$

$$\frac{a_1}{b_1}=\frac{a_2}{b_2}$$

□

אלגוריתם יעיל למצוא (רץ ב poly(lg(N))) שמוצא את השבר הנ"ל

האלגוריתם נקרא continued fraction
ועובד כך: מקבלים את θ ו-r ספרות אחרי הנקודה
ומציגים אותה כ- שלם + $\frac{1}{\text{שלם}}$

וממשיכים רקורסיבית עם השלם המכנה
עד שנשאר 0 + שלם.

מסתבר שאם הפעולה בשלב המסר מתקיימת אז כל האפשרויות ניקח ...

$$0.1385 = 0+\frac{1}{\frac{1}{0.1385}} = 0+\frac{1}{7.22022} = \frac{1}{7+0.22022} = \frac{1}{7+\frac{1}{\frac{1}{0.22}}}$$

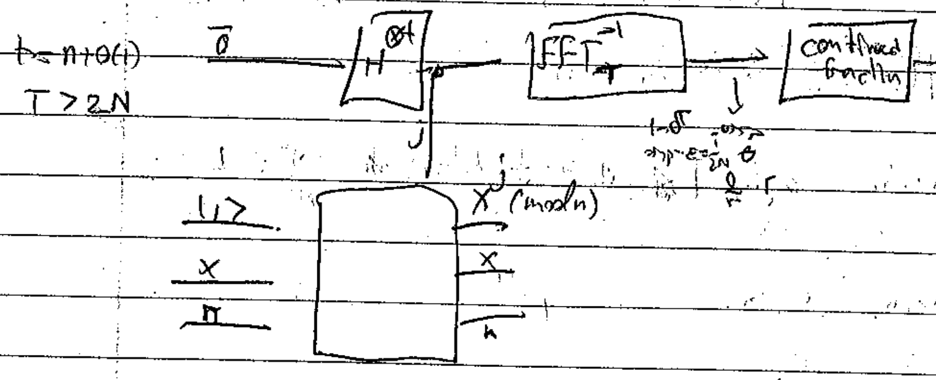
$$= \frac{1}{7+\frac{1}{4.54091}} = \frac{1}{7+\frac{1}{4.54091}} = \frac{1}{\ldots}$$

$\theta \approx 0.1385$

$$\theta = \frac{1}{\frac{1}{\theta}} = \frac{1}{7.22022} = \frac{1}{7+0.22022} = \frac{1}{7+\frac{1}{4.54091}} =$$

$$= \frac{1}{7+\frac{1}{4+\frac{1}{1.84874}}} = \frac{1}{7+\frac{1}{4+\frac{1}{1+1.17822}}}$$

וכך הלאה, עוצרים בשלב מסוים (לפי הדיוק) ומקבלים
את השבר המקורב



רוצים שמ' אחד r (מקסימלי קטן)
נקבל θ קרוב $\frac{1}{N^2}$ אל $\frac{l}{r}$
ואז נקבל את השבר $\frac{l}{r}$

כש l שלם זר ל r ($\gcd(l,r)=1$)

l זר ל r

בהסת.

ואז נקבל את r

המנגנון המקסימלי שעושים (...) הוא ההשוואה.

רדוקציה קוונטית (הסתברותית) מ factoring ל order finding

נתון n.

בחר אקראי $1 < x < n$.

א) $\gcd(x,n) > 1$. מצאנו גורם של n.

ב) n זוגי או חזקה של ראשוני - יודעים לפרק

ג) טענה: $\Pr\left[ord(x) = r \text{ זוגי ו } x^{\frac{r}{2}} \neq \pm 1 \right] \geq \frac{3}{8}$

הוכחה (רק בשביל זוג) n מכפלה של 2 ראשוניים שונים p, q אי זוגיים

נניח $n = p \cdot q$

לבחור x אקראי, זה כמו לבחור

x_1 אקראי מ $0..p-1$

x_2 " " $0..q-1$

ויחד הם x כך

$x \bmod p = x_1$

$x \bmod q = x_2$

לפי משפט השארית הסיני.

נ"ל $r_1 = ord(x_1)$ ב $\mathbb{Z}_p$

$r_2 = ord(x_2)$ ב $\mathbb{Z}_q$

אז $r = ord(x) = lcm(r_1, r_2)$

(מכאן) $r_1 | r$ ו $r_2 | r$

טענה! אם g יוצר של $\mathbb{Z}_p^*$, $x_1 = g^{a_1}$

אז $g^{a_1 \cdot r_1} = 1 = g^0 \pmod p$ ולכן $a_1 \cdot r_1 = 0 \pmod{p-1}$

$p-1$ זוגי, ולכן a_1 אי-זוגי $\Rightarrow$ r_1 זוגי.

קורה בהסתברות $\frac{1}{2}$.

כן a_2 זוגי-אי־זוגי ⇐ r_2 זוגי

קורה ב:
קורה ב-$\frac{1}{2}$

וכן a_1 וגם a_4 זוגי ⇐ r_1 גם כן זוגי או r זוגי.

קורה בהסת׳ $\frac{3}{4}$

<u>תרגיל:</u> $x^r = 1$

r זוגי: $x^{\frac{r}{2}}$

מקיים

$x^r(q)=1$, $x^r(p)=1$

ולכן $x^{r/2}(q)=\pm1$ $x^{\frac{r}{2}}(p)=\pm1$

וכל 4 האפשרויות מופיעות באותה (בערך) (סנוף הוכחה)

לכן בהסת׳ $\frac{1}{4}$ $x^{\frac{r}{2}}(n)\neq\pm1$

ולסיכום בהסת׳ $\frac{3}{4}\cdot\frac{1}{2}=\frac{3}{8}$ r זוגי ו $x^{\frac{r}{2}}\neq\pm1$. מ.ש.

נניח שמצאנו איזה w ש $w^2 \equiv 1$, $w \not\equiv \pm 1$

$(w+1)(w-1) \equiv 0 \pmod{n}$

$w \not\equiv 1 \ (n)$

$w \not\equiv -1 \ (n)$

אזי $\gcd(w+1, n) > 1$

או $\gcd(w+1, n) > 1$

מפרקים את n.