Feb. 16. 2011 (1)

Shor's algorithm

Course at the IUM by Christophe PITTET (I)

- n digit numbers

Any positive integer N can be written in a unique way

$$N = \sum_{k=0}^{n-1} a_k \cdot 2^k$$

where $a_k \in \{0;1\}$, $n \in \mathbb{N}$.

$N = (a_0, a_1, \ldots, a_{n-1})$, for example
$3 = (1,1)$ is 2-digit
$8 = (0,0,0,1)$ is 4-digit
$1023 = 2^{10} - 1$ is a 10-digit number

- Shor (1994): There is a probabilistic algorithm which factors an n-digit number $0 \leq N \leq 2^n - 1$ in less than

$$O(n^2 \cdot \log n \cdot \log\log n)$$

quantum steps.

- The goal of the course is to give the mathematical definition of a quantum step and to prove a bound of the type $O(n^4)$ for Shor's algorithm.

Proposition (Chinese remainder)

Let $N > 1$ be an integer

$$N = \prod_{p \in \mathcal{P}} p^{v_p(N)} \quad , \ \mathcal{P} \text{ set of primes}$$

$v_p(N)$ <u>valuation of N at p</u>

($v_p(N) = 0$ except for a finite number of primes p.

$v_2(8) = v_2(24) = 3$,

$v_p(M \cdot N) = v_p(N) + v_p(M) \quad \forall N, M \in \mathbb{N}, \ \forall p \in \mathcal{P}$)

$$\begin{tikzcd}
\mathbb{Z}/N\mathbb{Z} \arrow[r, "\substack{\text{isom.}\\ \text{of rings}\\ \sim}"] & \prod_{p \in \mathcal{P}} \mathbb{Z}/p^{v_p(N)}\mathbb{Z} \\
(\mathbb{Z}/N\mathbb{Z})^* \arrow[u, hook] \arrow[r, "\sim"] & \prod_{p \in \mathcal{P}} \left(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}\right)^* \arrow[u, hook]
\end{tikzcd}$$

isom.
of abelian groups
with multiplicative
notation.

Proof. Let $a, b > 1$ be integer and assume $(a,b) = 1$ (that is the greatest common divisor of a and b is 1

$(2,3) = 1$, $(6,12) = 6$).

$$\mathbb{Z}/_{a \cdot b}\mathbb{Z} \longrightarrow \mathbb{Z}/_{a}\mathbb{Z} \times \mathbb{Z}/_{b}\mathbb{Z}$$

$$x \longmapsto (x \ , \ x)$$

is a well-defined ring homomorphism if a/x (a divises x i.e. $x \equiv 0\,[a]$ i.e. $x \equiv 0$ in $\mathbb{Z}/_a\mathbb{Z}$) and $b/x \underset{(a,b)=1}{\Longrightarrow} ab/x$ that is $x \equiv 0$ in $\mathbb{Z}/_{ab}\mathbb{Z}$. Hence the above homomorphism is one-to-one, hence as

$$\left|\mathbb{Z}/_{ab}\mathbb{Z}\right| = ab = \left|\mathbb{Z}/_{a}\mathbb{Z} \times \mathbb{Z}/_{b}\mathbb{Z}\right|$$

it is a bijection.

It follows that

$$\mathbb{Z}/_{N}\mathbb{Z} \xrightarrow{\sim} \prod_{p \in \mathcal{P}} \mathbb{Z}/_{p^{v_p(N)}}\mathbb{Z}$$

$\left(\mathbb{Z}/N\mathbb{Z}\right)^*$ <u>is the set of elements of $\mathbb{Z}/N\mathbb{Z}$ which have an inverse for the multiplication.</u>

$x \in \mathbb{Z}/N\mathbb{Z}$ has an inverse

$$\Longleftrightarrow \quad (x, N) = 1$$

$\uparrow$
(Bezout).

The <u>Euler function</u> is by definition

$$\varphi(N) \doteq \left| \left(\mathbb{Z}/N\mathbb{Z}\right)^* \right|$$

$\varphi(N) =$ the number of elements $0 \leq x < N$ which are prime to N.

If A, B are commutative rings with units then

$$(A \times B)^* \cong A^* \times B^* \quad \text{because}$$

$$(a, b)^{-1} = (a^{-1}, b^{-1}) .$$

This finishes the proof of the proposition. ∎

<u>Proposition</u> (Units in a finite field form a cyclic group)

1) $\forall N \in \mathbb{N}, \quad N = \sum_{d | N} \varphi(d)$

2) Let K be a finite field then $K^* = K \setminus \{0\}$ is a cyclic group

3) $(\mathbb{Z}/_{p\mathbb{Z}})^*$ is cyclic of order $p-1$.

<u>Proof</u>

1) Let d be an integer. An element of $C_d \doteq \mathbb{Z}/d\mathbb{Z}$ is a generator of C_d $\overset{\text{Bezout}}{\iff}$ it is prime to d. Hence they are $\varphi(d)$ elements of order d in C_d.

There is a unique subgroup $C_d \cong \mathbb{Z}/_{d\mathbb{Z}}$ in $\mathbb{Z}/_{N\mathbb{Z}}$ if and only if $d | N$. It contains all the elements of $\mathbb{Z}/N\mathbb{Z}$ which are of order d. Hence

$$N = \sum_{d | N} \varphi(d)$$

2) $$\sum_{d \mid N} \varphi(d) = N \doteq |K^*| = \sum_{d \mid N} \underbrace{\left|\left\{ \begin{array}{c} \text{elements of } K^* \\ \text{of order } d \end{array} \right\}\right|}_{\overset{\wedge}{\varphi(d)}}$$

if $x \in K^*$ is of order d
then it is a root of $X^d - 1 \in K[X]$
but $\langle x \rangle \cong C_d$ contains all
the roots and contains $\varphi(d)$ elements
of order d.

Hence, $\forall\, d \mid N$,

$$\left|\left\{ \begin{array}{c} \text{elements of } K^* \\ \text{of order } d \end{array} \right\}\right| = \varphi(d) .$$

As $\varphi(N) > 0$, there is an element
of order N . i.e. K^* is cyclic.

3) $\mathbb{Z}/p\mathbb{Z}$ is a field because any
$0 < x < p$ is prime to p.

Hence according to 2)
$(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

$\blacksquare$

<u>Proposition</u> Let p be a prime and $m \in \mathbb{N}$.

1) $\varphi(p^m) = p^{m-1}(p-1)$.

2) If $p \neq 2$ then $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^*$ is cyclic

<u>Proof</u> 1) The elements of $\mathbb{Z}/p^m\mathbb{Z}$ which are not prime to p^m are the multiple of p:

$0, p, 2p, \dots, (p^{m-1}-1)p$.

Hence $p^m - p^{m-1}$ are prime to p^m

$\Rightarrow \varphi(p^m) = p^{m-1}(p-1)$.

2)
$$\begin{tikzcd}
\mathbb{Z}/p^m\mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/p\mathbb{Z} \\
\left(\mathbb{Z}/p^m\mathbb{Z}\right)^* \arrow[u, hook] \arrow[r, "\pi_*"] & \left(\mathbb{Z}/p\mathbb{Z}\right)^* \arrow[u, hook]
\end{tikzcd}$$

π_* is by definition the restriction of π to $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^*$

$\operatorname{Ker} \pi = \{0, p, 2p, \dots, (p^{m-1}-1)p\}$

$\operatorname{Ker} \pi_* = \{1, 1+p, 1+2p, \dots, 1+(p^{m-1}-1)p\}$

Hence $\operatorname{Ker} \pi_*$ is a subgroup of $\left(\mathbb{Z}/p^m\mathbb{Z}\right)^*$ with p^{m-1} elements.

$\left(\mathbb{Z}/8\mathbb{Z}\right)^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

<u>Claim</u>: $\operatorname{Ker} \pi_*$ is cyclic with generator $1+p$.

<u>Subclaim</u>: Let p be a prime, $p \neq 2$, let $e \in \mathbb{N}$, then

$$(1+p)^{p^e} \equiv 1 + p^{e+1} \quad [p^{e+2}]$$
$$(1+2)^{2^2} \not\equiv 1 + 2^{2^2} \quad [2^3]$$

<u>Proof of the subclaim</u>: if $e = 0$ it is obvious.

$$(1+p)^{p^{e+1}} = \left((1+p)^{p^e}\right)^p = \quad \begin{pmatrix}\text{induction} \\ d \in \mathbb{N}\end{pmatrix}$$

$$= \left(1 + p^{e+1} + d\,p^{e+2}\right)^p$$

$$= \left(1 + p^{e+1}(1+dp)\right)^p$$

$$= 1 + p^{e+2}(1+dp) + \sum_{k=2}^{p-1} \binom{p}{k} p^{k(e+1)} (1+dp)^k$$
$$+ p^{p(e+1)}(1+dp)^p$$

$$\equiv 1 + p^{e+2} \quad [p^{e+3}]$$

$\uparrow$

$p \mid \binom{p}{k} \quad 1 \leq k \leq p-1$

$k(e+1)+1 \geq e+3$ if $k \geq 2$

and $p(e+1) \geq e+3$ if $p \geq 3$.

End of the proof of the subclaim

$\blacksquare$

<u>Proof of the claim</u>: the order of $1+p$ in $\operatorname{Ker}\bar{\pi}_*$ divides $|\operatorname{Ker}\bar{\pi}_*| = p^{m-1}$.
Hence order $(1+p) = p^e$ with $e \leq m-1$.
We want to show that $e \geqslant m-1$.
We have:

$$1+p^{e+1}+dp^{e+2} \underset{\uparrow}{=} (1+p)^{p^e} \underset{\uparrow}{\equiv} 1\ [p^m] .$$

subclaim — order $(1+p)$ is p^e in $(\mathbb{Z}/p^m\mathbb{Z})^*$

Hence

$$p^m \mid p^{e+1}(1+dp) .$$

Hence $p^m \mid p^{e+1}$ i.e. $m \leqslant e+1$.
End of the proof of the claim ∎.

<u>Lemma</u>: Let G be a group, let $x,y \in G$ be two elements which commute ($[x,y] = xyx^{-1}y^{-1} = 1$):
If the order $o(x)$ of x and the order $o(y)$ of y are finite and relatively prime, then
$o(xy) = o(x) \cdot o(y)$.

Proof of the lemma:

let $d \in \mathbb{N}$ s.t. $(xy)^d = 1$ then as $[x,y]=1$, $x^d = y^{-d}$. Hence the order of x^d divides the order of y (as $x^d \in \langle y \rangle$) and the order of y^{-d} divides the order of x. As $(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$, the order of $x^d = y^{-d}$ is 1: that is $x^d = y^{-d} = 1$.

Hence d is a multiple of the order of x and of the order of y. As $(\mathrm{ord}(x), \mathrm{ord}(y)) = 1$, d is a multiple of $\mathrm{ord}(x) \cdot \mathrm{ord}(y)$. On the other hand,

$$(xy)^{\mathrm{ord}(x) \cdot \mathrm{ord}(y)} \underset{[x,y]=1}{=} x^{\mathrm{ord}(x)\,\mathrm{ord}(y)}\, y^{\mathrm{ord}(x)\,\mathrm{ord}(y)}$$

$$= \left(x^{\mathrm{ord}(x)}\right)^{\mathrm{ord}(y)} \cdot \left(y^{\mathrm{ord}(y)}\right)^{\mathrm{ord}(x)} = 1$$

End of the proof of the lemma ∎.

End of the proof of (2) in the proposition:

we have seen the map $(\mathbb{Z}/p^m\mathbb{Z})^* \xrightarrow{\pi_*} (\mathbb{Z}/p\mathbb{Z})^*$ has kernel $C_{p^{m-1}}$ generated by $1+p$.

As $|(\mathbb{Z}/p^m\mathbb{Z})^*| = p^{m-1}(p-1)$ and $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$ we deduce that π_* is surjective.

Let σ be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ and let $\tilde{\sigma} \in (\mathbb{Z}/p^m\mathbb{Z})^*$: $\pi_*(\tilde{\sigma}) = \sigma$. Let d be order of $\tilde{\sigma}$. We have $\sigma^d = 1$ hence $\exists\, k : (p-1)k = d$.
The order of $\tilde{\sigma}^k$ is $p-1$.
Hence the order of $(1+p)\cdot\tilde{\sigma}^k$ is $p^{m-1}\cdot(p-1)$. This shows that $(1+p)\cdot\tilde{\sigma}^k$ generates $(\mathbb{Z}/p^m\mathbb{Z})^*$. ∎

<u>Proposition</u> (First step in Shor's algorithm: reducing the factorization problem to the period finding problem.)

Let $N > 1$ be an integer. Let us pick an integer $y < N$ which is prime to N : $(y, N) = 1$.

1) The period of the function
$$\exp_y : \mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$$
$$x \longmapsto y^x$$
equals the order of y in $(\mathbb{Z}/N\mathbb{Z})^*$.

2) If the period r of $\exp_y$ is even and if $y^{r/2}+1$ is not equal to zero in $\mathbb{Z}/N\mathbb{Z}$, then
$$1 < \gcd(N, y^{r/2}-1) < N .$$

Proof of the proposition

1) Let r be the order of $y \in \left(\mathbb{Z}/N\mathbb{Z}\right)^*$; that is r is the smallest integer such that

$$y^r = \exp_y(r) = 1 .$$

Hence r is the smallest integer s.t.

$$\exp_y(x+r) = \exp_y(x) \quad \forall\, x \in \mathbb{Z} .$$

2) As r is even we have the identity

$$(y^{r/2}-1)(y^{r/2}+1) = y^r - 1 .$$

Hence

$$N \text{ divides } (y^{r/2}-1)\cdot(y^{r/2}+1) .$$

As N does not divide $y^{r/2}+1$ by hypothesis, at least one of the prime factor of N must divide $y^{r/2}-1$. Hence

$$1 < \gcd(N, y^{r/2}-1) .$$

On the other hand, N does not divide $y^{r/2}-1$ by minimality of the order r of y. Hence

$$\gcd(N, y^{r/2}-1) < 1 .$$

<u>Addendum to Proposition p. 7</u>

p prime, $p \neq 2$, $\varphi \doteq |(\mathbb{Z}/p^m\mathbb{Z})^*| = p^{m-1}(p-1)$ is even.

Let σ be a generator of $(\mathbb{Z}/p^m\mathbb{Z})^*$

Let v_2 be the valuation at 2. Let $k = 0, 1, \dots, \varphi/2 - 1$.

Then

$$v_2(\mathrm{order}(\sigma^{2k})) < v_2(\mathrm{order}(\sigma))$$

$$v_2(\mathrm{order}(\sigma^{2k+1})) \geq v_2(\mathrm{order}(\sigma)).$$

Hence the above inequalities splits $(\mathbb{Z}/p^m\mathbb{Z})^*$ in two halfs.

<u>Proof of the addendum</u>: As φ is even, $(\sigma^{2k})^{\varphi/2} = (\sigma^{\varphi})^k = 1$ hence the order of σ^{2k} divides $\varphi/2$. This proves $v_2(\mathrm{order}(\sigma^{2k})) < v_2(\varphi)$.

Let d such that $(\sigma^{2k+1})^d = 1$.

Hence $\varphi \mid (2k+1)\cdot d$. This implies

$$v_2(\varphi) \leq v_2((2k+1)\cdot d) = v_2(2k+1) + v_2(d) = v_2(d)$$

■

<u>Lemma</u> Let $N > 1$ be an odd number, that is

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

$\alpha_i > 0$, $m \geq 1$, $p_i \neq 2$. Let

$$S = \{ y \in (\mathbb{Z}/N\mathbb{Z})^* : \text{the order } r \text{ of } y \text{ is even } \underline{\text{and}}\ y^{r/2} + 1 \neq 0 \}.$$

Then $|S| \geq \varphi(N)\left(1 - 1/2^{m-1}\right)$.

Hence, if N is odd and not a prime power (i.e. $m \geq 2$) at least half of $(\mathbb{Z}/N\mathbb{Z})^*$ falls in S.

<u>Proof:</u> Let $F = (\mathbb{Z}/N\mathbb{Z})^* \setminus S$, that is $y \in (\mathbb{Z}/N\mathbb{Z})^*$ is in F if and only <u>either</u> the order r of y is odd <u>or</u> $y^{r/2} + 1 = 0$.

<u>Claim 1:</u> if $y \in F$ then

$$v_2(\text{order}(y)) = v_2(\text{order}(y_i))$$

$\forall\, i = 1, \ldots, m$ where

$$(\mathbb{Z}/N\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_m^{\alpha_m}\mathbb{Z})^*$$

$$y \longmapsto (y_1, \ldots, y_m)$$

<u>Proof of Claim 1:</u>

Let r be the order of y in $(\mathbb{Z}/N\mathbb{Z})^*$ and let r_i be the order of the component y_i of y in the above isomorphism.

$1 = y^r = (y_1^r, \dots, y_m^r)$ hence

$y_i^r = 1$ hence $r_i \mid r$, hence

$v_2(\text{order}(y_i)) \leq v_2(\text{order}(y))$.

If the order r of y is odd then $v_2(\text{order}(y)) = 0$. Hence the above inequality implies

$v_2(\text{order}(y_i)) = 0$ also.

If r is even but $y^{r/2} = -1$ in $(\mathbb{Z}/N\mathbb{Z})^*$ then $y_i^{r/2} = -1$ in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ for each $i = 1, \dots, m$.

Hence r_i does not divide $r/2$ ($-1 \neq 1$ because $p_i \neq 2$) hence

$v_2(r_i) = v_2(r)$ (recall $r_i \mid r$).

End of the proof of Claim 1 ■

Claim 2

$$\left| \left\{ y \in (\mathbb{Z}/N\mathbb{Z})^* : \begin{array}{c} v_2(\text{order}(y)) = v_2(\text{order}(y_i)) \\ \forall i = 1, \dots, m \end{array} \right\} \right|$$

$$\leq \varphi(N)/2^{m-1}.$$

Proof of claim 2:

Let $y_1 \in (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^*$. For each $i = 2, \dots, m$ there is at most $\varphi(p_i^{\alpha_i})/2$ elements y_i in $(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^*$ s.t.

$v_2(\text{order}(y_i)) = v_2(\text{order}(y_1))$ according to the addendum to Prop. p. 7.

Hence there are at most

$$\prod_{i=2}^{m} \frac{\varphi(p_i^{\alpha_i})}{2} \quad \text{elements of} \quad \left(\mathbb{Z}/_{N\mathbb{Z}}\right)^*$$

such that $v_2(\text{order}(y_1)) = v_2(\text{order}(y_i))$ $\forall\, i \geq 2$.

Summing over all elements of $\left(\mathbb{Z}/_{p_1^{\alpha_1}}\right)^*$

we obtain at most

$$\varphi(p_1^{\alpha_1}) \cdot \prod_{i=2}^{m} \frac{\varphi(p_i^{\alpha_i})}{2} = \frac{\varphi(N)}{2^{m-1}}. \quad \blacksquare$$