

# IQI 04, Seminar 9

Produced with pdflatex and xfig

- Factoring algorithms.
- Quantum order finding.
- Quantum Fourier transform.

E. "Manny" Knill: [knill@boulder.nist.gov](mailto:knill@boulder.nist.gov)



TOC

## Composite and Prime Numbers

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ , the set of natural numbers.
  - $f|n$  means  $f$  divides  $n$ .
  - $f$  is a *proper factor* of  $n$  if  $1 < f < n$  and  $f|n$ .
  - $p$  is a prime if  $1 < p$  and  $p$  has no proper factors.
- Examples:
- Primes: 2, 3, 5, 7, 11, 13, 17, ...
  - What divides 15?  $15 = 3 * 5$  so  $3|15, 5|15$ .
  - Which of the following are prime?

23 : prime

21 :  $3 * 7$

47 : prime

51 :  $3 * 17$

91 :  $7 * 13$



1  
TOC

## Factoring

- The factoring problem:

Given:  $N \in \mathbb{N}, N > 1, N$  not a prime.

Problem: Write  $N$  as a product  $N = p * q, p > 1, q > 1$ .

- Examples:

49 :  $49 = 7 * 7$

24 :  $24 = 8 * 3 = 4 * 6 = \dots = 2^3 * 3$

42 :  $42 = 2 * 21 = 6 * 7 = \dots = 2 * 3 * 7$

- Input size: Number of binary digits of  $N, n = \lfloor \log_2(N) \rfloor + 1$ .

- Complexity of factoring.

- Best classical algorithm:  $\simeq e^{1.93 \ln(N)^{1/3} \ln \ln(N)^{1-1/3}}$

Number field sieve, complexity based on number density heuristics.

Note: This is *subexponential* but *superpolynomial*.

- Best quantum algorithm:  $\tilde{O}(n^2)$ .

Shor's algorithm.  $\tilde{O}(f(n))$  means that for some  $k, O(f(n) \log(n)^k)$

2  
TOC

## Trial Division Algorithm

- TRIALDIVISIONFACTOR( $N$ )

**Input:**  $N > 1$

**Output:** If  $N$  is prime, 1, else a proper factor  $f$  of  $N$ .

for  $f = 2$  to  $\lfloor \sqrt{N} \rfloor$

if  $f|N$  then return  $f$

end

return 1

- Complexity:  $\lfloor \sqrt{N} \rfloor - 1$  trial divisions in the worst case.

If  $f$  is the smallest factor, it requires  $f - 1$  trial divisions.

- Division with remainder:

**Input:**  $1 \leq f < g$

**Output:**  $\lfloor \frac{g}{f} \rfloor$  and the remainder  $g \% f = g - \lfloor \frac{g}{f} \rfloor f$

- Complexity:  $O(\log(g)^3)$  for long division,

$\tilde{O}(\log(g)^2)$  for the best algorithm known.

3  
TOC

## Modular Arithmetic

- $\mathbb{Z}_q = \{0, \dots, q-1\}$  with modular addition, multiplication rules:

1. Add/multiply as integers,
2. then *reduce modulo q* (remainder after division by  $q$ ).

**Notation:**  $a \bmod q = a \% q$ .  $a = b \bmod q$  means  $a \% q = b \% q$ .

**Example:**  $16 = 9 = 2 \bmod 7$ .

- Modular identities:

$$f + g = f \% q + g \% q \bmod q$$

$$f + g = d_f * q + f \% q + d_g * q + g \% q = f \% q + g \% q + (d_f + d_g) * q$$

$$f * g = (f \% q) * (g \% q) \bmod q$$

$$f * g = (d_f * q + f \% q) * (d_g * q + g \% q) = (f \% q) * (g \% q) + (\dots) * q$$

- $\mathbb{Z}_q$  with addition and multiplication modulo  $q$  is a *ring*.

4  
TOC

## Largest Common Divisors

- The largest common divisor  $\gcd(f, g)$  of  $f$  and  $g$  is the maximum  $d$  such that  $d|f$  and  $d|g$ .

- EUCLID( $f, g$ )

**Input:**  $f > g > 1$

**Output:**  $d, k, l \in \mathbb{Z}$  such that  $kf + lg = \gcd(f, g) = d$ .

$$f_1 \leftarrow f; k_1 \leftarrow 1; l_1 \leftarrow 0$$

$$f_2 \leftarrow g; k_2 \leftarrow 0; l_2 \leftarrow 1$$

**C:** Each  $f_c$  is divisible by  $d$ . The last non-zero  $f_c$  is equal  $d$ .

$$c = 0;$$

**repeat**

$$c \leftarrow c + 1;$$

$$x \leftarrow \lfloor f_c / f_{c+1} \rfloor$$

$$f_{c+2} \leftarrow f_c \% f_{c+1};$$

$$(* f_{c+2} = f_c - x f_{c+1} \Rightarrow d | f_{c+2}. *)$$

$$k_{c+2} \leftarrow k_c - x k_{c+1}$$

$$l_{c+2} \leftarrow l_c - x l_{c+1}$$

**until**  $f_{c+2} = 0$

**return**  $f_{c+1}, k_{c+1}, l_{c+1}$

**Example:**  $f = 132, g = 111$ .

$$\begin{array}{rcl} f_1 = 132 & = & 1 * f + 0 * g \\ f_2 = 111 & = & 0 * f + 1 * g & x=1 \\ f_3 = 21 & = & 1 * f - 1 * g & x=5 \\ f_4 = 6 & = & -5 * f + 6 * g & x=3 \\ f_5 = 3 & = & 16 * f - 19 * g & x=2 \\ f_6 = 0 & & & \end{array}$$

5  
TOC

## The Structure of $\mathbb{Z}_q$

- $a$  is *relatively prime* to  $q$ ,  $(a, q) = 1$ , if  $\gcd(a, q) = 1$ .

- If  $(a, q) = 1$ , then for some  $b$ ,  $ba = 1 \bmod q$ .

**Proof.** Choose  $k, l$ , such that  $ka + lq = 1$ . Then  $b = k \bmod q$ .

-  $a$  is invertible mod  $q$ , so write  $b = a^{-1} \bmod q$ .

**Example:**  $q = 21, a = 5$ . Then  $17 * 5 = 85 = 1 \bmod 21$ .

- $(a, q) = 1$  and  $(b, q) = 1$  implies  $(a * b, q) = 1$ .

- The set  $\mathbb{Z}_q^* = \{a \mid (a, q) = 1\}$  is a group under multiplication.

- Euler  $\phi$  function:  $\phi(q) = |\mathbb{Z}_q^*|$ .

**Examples:** -  $\phi(6) = 2$  because 1, 5 are relatively prime to 6.

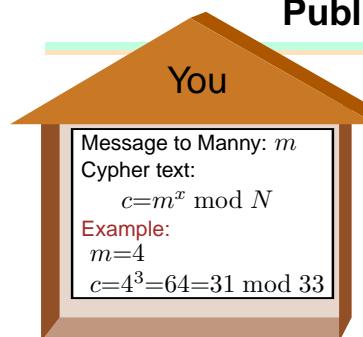
- For  $p$  a prime,  $\phi(p) = p - 1$ .

- For  $a \in \mathbb{Z}_q^*$ ,  $a^{\phi(q)} = 1 \bmod q$ .

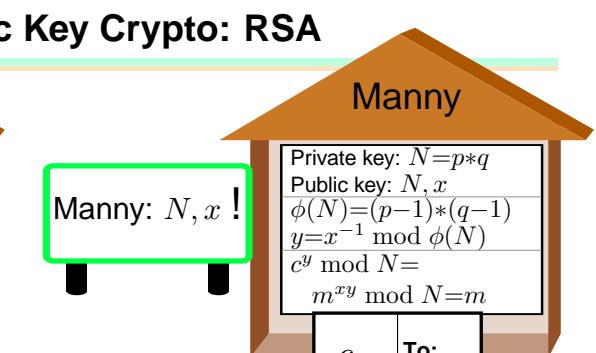
**Proof.** Basic group theory.

6  
TOC

## Public Key Crypto: RSA



$$\begin{aligned} 31 &= -2 \bmod 33 \\ (-2)^2 &= 4 \bmod 33 \\ (-2)^4 &= 4^2 \\ &= 16 \bmod 33 \\ (-2)^7 &= -2 * 4 * 16 \bmod 33 \\ &= -2 * 64 \bmod 33 \\ &= -2 * 31 \bmod 33 \\ &= -62 \bmod 33 \\ &= 4 \bmod 33 \end{aligned}$$



- Pick two large primes  $p, q$ .

$$N = p * q$$

$$\phi(N) = (p - 1) * (q - 1)$$

$$x = x^{-1} \bmod \phi(N)$$

$$y = 3^{-1} = 7 \bmod \phi(N)$$

- Order of  $m$  is  $\phi(N)$ !

$$p=3, q=11$$

$$N=33$$

$$\phi(33)=2 * 10=20$$

$$x=3$$

$$y=3^{-1}=7 \bmod \phi(N)$$

$$c^y=31^7 \bmod N$$

$$= 31 * 31^2 * 31^4 \bmod N$$

7  
TOC

## Factor Finding with Square Roots of Unity

- Let  $N$  be composite.
- Find  $x$  such that  $x^2 \equiv 1 \pmod{N}$  and  $x \not\equiv \pm 1 \pmod{N}$ .
  - $x^2 - 1 = (x - 1)(x + 1) \equiv 0 \pmod{N}$ .
  - Hence either  $N > \gcd(x - 1, N) > 1$  or  $N > \gcd(x + 1, N) > 1$ .
  - $N$  can be factored.
  - $x$  is a non-trivial square root of unity modulo  $N$ .
- Suppose  $N$  is odd, not a prime power.  
Then nontrivial square roots of unity modulo  $N$  exist.
- Examples:  
 $N = 15$ .  $\sqrt{1} \pmod{15}$ : 1, 4, 11, 14.  $\gcd(4 - 1, 15) = 3$ ,  $\gcd(4 + 1, 15) = 5$ .  
 $N = 35$ .  $\sqrt{1} \pmod{35}$ : 1, 6, 29, 34.  $\gcd(29 - 1, 35) = 7$ ,  $\gcd(29 + 1, 35) = 5$ .
- Easy to factor:  $\begin{cases} \text{Even numbers: } N = 2M. \\ \text{Power numbers: } N = M^k, k > 1 \end{cases}$

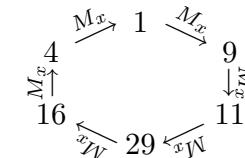
8  
TOC

## Quantum Order Finding

- Problem:** Given  $N, x, (x, N) = 1$ .  $\text{ORDER}(x \pmod{N})$ ?
- Consider  $M_x : y \mapsto x * y \pmod{N}$ . Let  $o = \text{ORDER}(x \pmod{N})$ .
  - $M_x$  is invertible on  $\mathbb{Z}_N^*$ .
  - $M_x$ 's cycles on  $\mathbb{Z}_N^*$  are of length  $o$ .

$$1 \xrightarrow{M_x} x \xrightarrow{M_x} x^2 \xrightarrow{M_x} \dots \xrightarrow{M_x} x^{o-1} \xrightarrow{M_x} 1$$

Example:  $N = 35, x = 9, o(x) = 6$ .



- $M_x^k = M_{x^k}$  is efficiently implementable. To compute  $x^k$ :
  - Write  $k = k_0 k_1 \dots k_b$  in reverse binary.
  - Compute  $x^{2^j} \pmod{N}$ ,  $j = 0, \dots, b$  by repeated squaring.
  - $x^k = x^{k_0 2^0} \dots x^{k_b 2^b}$ .

10  
TOC

## From Order to Square Roots of Unity

FACTOR( $N$ )**Input:**  $N > 1$ ,  $N$  odd, not a prime power.**Output:** A nontrivial factor  $f$  of  $N$ .

```

 $f \leftarrow 1$ 
while  $f = 1$ 
   $x \leftarrow \text{rand}(2, N - 1); f \leftarrow \text{gcd}(x, N)$ 
  if  $f > 1$  then return  $f$ 
   $o \leftarrow \text{ORDER}(x \pmod{N})$ 
  if  $2|o$  &  $x^{o/2} \pmod{N} \notin \{1, -1\}$ 
     $f \leftarrow \max(\text{gcd}(x^{o/2} - 1, N), \text{gcd}(x^{o/2} + 1, N))$ 
  end
end
return  $f$ 

```

- Prob(  $1 < x < N$  has even order  $o$  and  $x^{o/2} \notin \{1, -1\}$  )  $\geq 1/2$ .

9  
TOC

## Quantum Order Finding

- Problem:** Given  $N, x, (x, N) = 1$ .  $\text{ORDER}(x \pmod{N})$ ?
- Consider  $M_x : y \mapsto x * y \pmod{N}$ . Let  $o = \text{ORDER}(x \pmod{N})$ .
  - $M_x$  is invertible on  $\mathbb{Z}_N^*$ , has cycles of length  $o$  and  $M_x^k$  is efficient.
- Quantum extension of  $M_x$ .
  - Let  $S$  be an  $n$ -qubit register,
  - Logical states:  $|0\rangle_s, \dots, |2^{n-1}\rangle_s$ ,  $2^n > N$ .
  - $M_x|y\rangle_s = |x * y \pmod{N}\rangle_s$  for  $0 \leq y < N$ .
  - $(M_x)^k \sum_{y=0}^{N-1} \alpha_y |y\rangle_s = \sum_{y=0}^{N-1} \alpha_y |x^k * y \pmod{N}\rangle_s$ .

Eigenvalues of  $M_x$ ?

Let  $\omega = e^{i\frac{2\pi}{o}}$ , abbreviate  $|m\rangle = |m \pmod{N}\rangle$  and define

$$\begin{aligned}
 |\psi_l\rangle_s &= \sum_{k=0}^{o-1} (\omega^{-l})^k |x^k\rangle && \dots \text{normalization of } \frac{1}{\sqrt{o}} \text{ omitted.} \\
 M_x|\psi_l\rangle_s &= \omega^l \left( \omega^{-l}|x^1\rangle + \dots + \omega^{-l(o-1)}|x^{o-1}\rangle + \omega^{-lo}|x^o\rangle \right) \\
 &= \omega^l (|x^0\rangle + \omega^{-l}|x^1\rangle + \dots + \omega^{-l(o-1)}|x^{o-1}\rangle) \\
 &= \omega^l |\psi_l\rangle
 \end{aligned}$$

11  
TOC

## From Eigenvalues to Order

- Given operators  $M_{x^k}|y\rangle = |x^k * y\rangle$ ,  $M_{x^k}|\psi_l\rangle = e^{i\frac{2\pi lk}{o}}|\psi_l\rangle$ . Determine  $o$ ?
  - Use phase estimation with input state  $|1\rangle$ .
- 
- $\tilde{r} = \left(\frac{l}{o}\right) \pm \epsilon$
- with  $\text{Prob}(l) = 1/o$
- Inferring  $o$  from  $\tilde{r}$ . Known:  $1 < o < N$ .
    - Determine  $p/q$  with  $q < N$  and  $|p/q - \tilde{r}|$  minimal.
      - Can be done efficiently by the *continued fraction algorithm*.
      - If  $\epsilon < 1/N^2$ ,  $q|o$  with high confidence.
    - Check whether  $o$  is the order of  $x$ .
    - If not, try phase estimation again.

12

TOC

## Efficient Phase Estimation

**PHASEEST( $P, k$ )**

**Input:** An unknown  $z$ -rotation  $P$ , with efficient  $P^{2^l}$ .

**Output:**  $\tilde{x} = .x_1 \dots x_k$ , the approximate angle of  $P$  in binary.

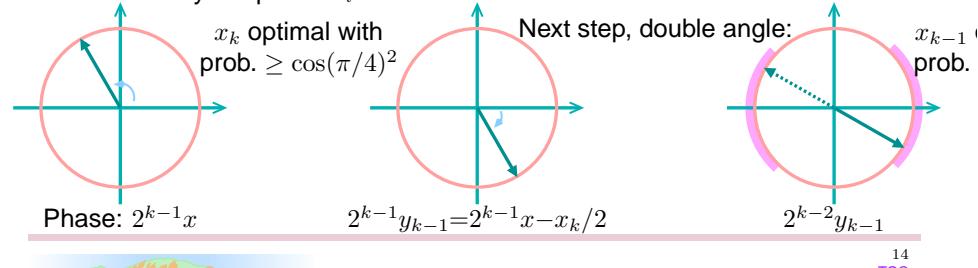
```

 $P_k \leftarrow P$ 
for  $l = k$  to 1
     $(P_{l-1}, x_l) \leftarrow \text{PHASESTEP}(P_l, l)$ 
end

```

- Analysis. Define  $P = e^{-ix\pi\sigma_z}$ ,  $P_l = e^{-iy_l\pi\sigma_z}$ .

Probability of optimal  $x_l$  for each  $l$ :



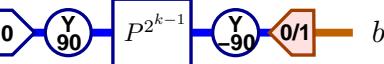
14

TOC

## A Phase Estimation Step

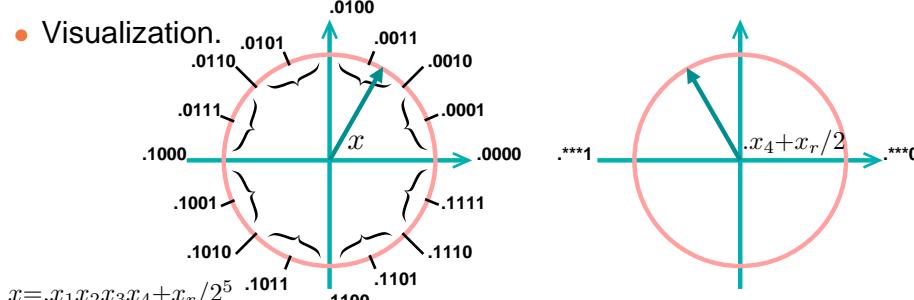
- PHASESTEP( $P, k$ )**
- Input:**  $k \geq 1$ , black box  $P = e^{-ix\pi\sigma_z}$ ,  $x$  unknown, efficient  $P^{2^l}$ .
- Output:** 1. Modified black box  $P' = e^{i\frac{b\pi}{2^k}\sigma_z}P$  for  $b = 0$  or  $b = 1$ .  
2.  $b$ , which approximates the  $k$ 'th bit of  $x$ .

1. Implement



2. Return  $P' = e^{i\frac{b\pi}{2^{k+1}}\sigma_z}P$ .

- Visualization.



13

TOC

## Efficient Phase Estimation

**PHASEEST( $P, k$ )**

**Input:** An unknown  $z$ -rotation  $P$ , with efficient  $P^{2^l}$ .

**Output:**  $\tilde{x} = .x_1 \dots x_k$ , the approximate angle of  $P$  in binary.

```

 $P_k \leftarrow P$ 
for  $l = k$  to 1
     $(P_{l-1}, x_l) \leftarrow \text{PHASESTEP}(P_l, l)$ 
end

```

- Analysis. Define  $P = e^{-ix\pi\sigma_z}$ ,  $P_l = e^{-iy_l\pi\sigma_z}$ .

Probability of optimal  $x_l$  for each  $l$ :  $\gtrsim .4$

The bound can be chained:

$$\text{Prob}(|\tilde{x} - x| \leq 1/2^k) \gtrsim .4.$$

$$\text{Prob}(|\tilde{x} - x| \leq 1/2^{k-1}) \gtrsim .4 + (.6) * .4 = .64$$

$$\text{Prob}(|\tilde{x} - x| \leq 1/2^{k-2}) \gtrsim .4 + (.6) * .4 + (.6)^2 * .4 = .78$$

$\vdots$

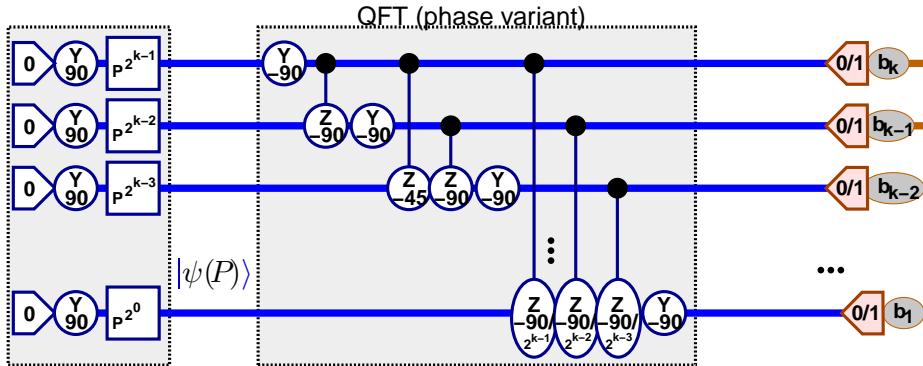
$$\text{Prob}(|\tilde{x} - x| \leq 1/2^{k-l}) \gtrsim 1 - .6^{l+1}$$

15

TOC

## Quantum Fourier Transform

- From the full phase estimation network to the QFT.



- If  $P = e^{-il\pi/2^k}$ , then  $|\psi(P)\rangle$  is the  $l$ 'th Fourier state modulo  $2^k$ . Hence QFT transforms Fourier states to logical states.

⇒ QFT is a phase variant of Fourier transform.

16  
TOC

## References

- [1] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26:1484–1509, 1997.
  - [2] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54:1034–, 1996.
  - [3] A. Ekert and R. Jozsa. Notes on quantum factoring. *Reviews of Modern Physics*, 68:733–753, 1996.
  - [4] M. E. Briggs. *An Introduction to the General Number Field Sieve*. PhD thesis, Virginia Polytechnic Institute and State University, Blacksburg, Virginia, 1998.
  - [5] A. K. Lenstra. Integer factoring. *Designs, Codes and Cryptography*, 19:101–128, 2000.

## Contents

Title: IQI 04, Seminar 9.....	.0	Quantum Order Finding I .....	.10
Composite and Prime Numbers .....	.1	Quantum Order Finding II .....	.11
Factoring .....	.2	From Eigenvalues to Order .....	.12
Trial Division Algorithm .....	.3	A Phase Estimation Step .....	.13
Modular Arithmetic .....	.4	Efficient Phase Estimation I .....	.14
Largest Common Divisors .....	.5	Efficient Phase Estimation II .....	.15
The Structure of $\mathbb{Z}_q$ .....	.6	Quantum Fourier Transform .....	.16
Public Key Crypto: RSA .....	.7	References .....	.18
Factor Finding with Square Roots of Unity .....	.8		
From Order to Square Roots of Unity .....	.9		

16  
TOC

18  
TOC