Einführung

Quantum Computing

HSK 8.1.2025

- **Factoring**
  - **Periodizität**
  - **Modulo Multiplikation**
  - **QPE**
  - **Implementierungsbeispiel**

Periodizität

Sei N das Produdkt der zwei Primzahlen $\boldsymbol{p}$ *und* $\boldsymbol{q}$

$$N = p \cdot q$$

Periodizität

Sei N das Produdkt der zwei Primzahlen $\boldsymbol{p}$ *und* $\boldsymbol{q}$

$$N = p \cdot q$$

$$f(x) = a^x \; mod \; \mathrm{N}$$

Periodizität p: $f(x) = f(x+p)$ $\forall\, x \in \mathbb{D}_f$

r *ist die Ordnung von* a *modulo* N *wenn*: $a^r \; mod \; N = 1$ $p = r$ $ggT(a, N) = 1$

Periodizität

$$N = p\ q$$

$$f(x) = a^x \ mod\ N \qquad\qquad ggT(a, N) = 1$$

$$r\ Periodizität\ von\ f\ und\ \boldsymbol{gerade}$$

$$ggT\left(\left(a^{r/2} - 1\right), N\right) = p$$

$$ggT\left(\left(a^{r/2} + 1\right), N\right) = q$$

Periodizität

$p = 7$
$q = 13$
$N = 91$
$a = 4$

$f(x) = a^x \ mod \ \mathrm{N}$ ⟶ $f(x) = 4^x \ mod \ 91$

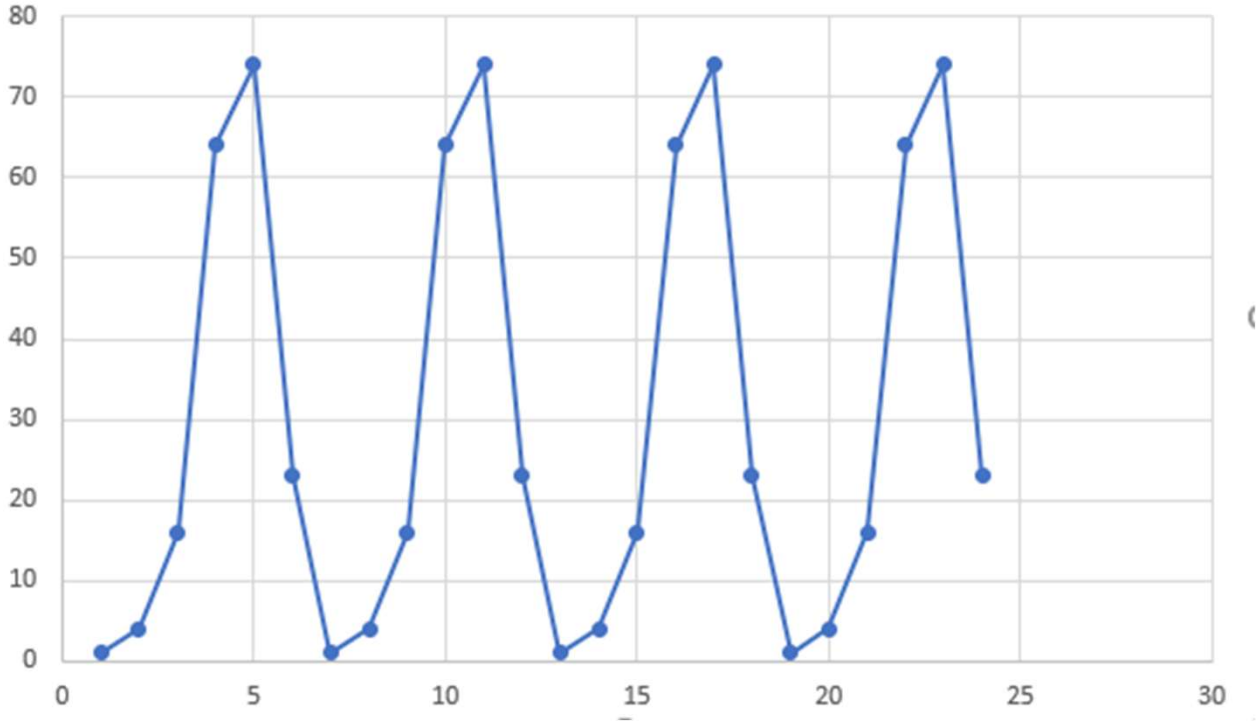
x: 0	f(x): 1
x: 1	f(x): 4
x: 2	f(x): 16
x: 3	f(x): 64
x: 4	f(x): 74
x: 5	f(x): 23
x: 6	f(x): 1
x: 7	f(x): 4
x: 8	f(x): 16
x: 9	f(x): 64
x: 10	f(x): 74
x: 11	f(x): 23
x: 12	f(x): 1
x: 13	f(x): 4

$$ggT\left(\left(a^{r/2} - 1\right), N\right) = ggT\left((4^3 - 1), 91\right) = ggT(63,91) = 7$$

$$ggT\left(\left(a^{r/2} + 1\right), N\right) = ggT\left((4^3 + 1), 91\right) = ggT(65,91) = 13$$

Periodizität

$$f(x) = 4^x \ mod \ 91$$



Modulare Multiplikation

$a, b, m \in \mathbb{Z}$:

$$r_a = a \pmod m$$

$$r_b = b \pmod m$$

$$(a \cdot b) \pmod m \equiv (r_a \cdot r_b) \pmod m$$

Beispiel :

$a = 47\,, b = 73\,, m = 15$

$$r_a = 47 \pmod{15} = 2$$

$$r_b = 73 \pmod{15} = 13$$

$$(47 \cdot 73) \pmod{15} = 3431 \pmod{15} = 11$$

$$(2 \cdot 13) \pmod{15} = 26 \pmod{15} = 11$$

Modulare Multiplikation

$$f(x) = a^x \; mod \; \mathrm{N}$$

$$x = x_0 \, 2^0 + x_1 \, 2^1 \quad \ldots x_{n-1} \, 2^{n-1}$$

$$(x_{n-1} \, , x_{n-2} \, , x_{n-3} \, , \ldots x_0 \,)_2$$

$$a^x \; mod \; \mathrm{N} = (\left(\left(\left((a^{x_0 \, 2^0} \; mod \; N) \cdot a^{x_1 \, 2^1} \; mod \; \mathrm{N} \right) \cdot a^{x_2 \, 2^2} \; mod \; N \right) \ldots \ldots \right) \cdot a^{x_{n-1} \, 2^{n-1}} \; mod)$$

Modulare Multiplikation

$U|y> = \ |ay \ mod \ N>$ $\qquad$ $y \ \in \ \{0, \dots, N-1\}$ $\qquad$ $n \ qBits \ \ 2^n \ \approx N$

$$U^0|1> = \ |1 \ mod \ N> = \ |a^0 \ mod \ N>$$

$$U^1|1> = \ |a \ mod \ N> = \ |a^1 \ mod \ N>$$

$$U^2|1> = \ |a^2 \ mod \ N>$$

$$\vdots$$

$$U^r|1> = \ |a^r mod \ N> = \ |a^0 \ mod \ N>$$

Modulare Multiplikation

$U|y> = \ |ay \ mod \ N>$ $\qquad\qquad$ $s \ \in \ \{0, \dots, r-1\}$

$|a^0 \ mod \ N> \qquad |a^1 \ mod \ N> \qquad |a^2 \ mod \ N> \qquad \cdots \qquad |a^{r-1} \ mod \ N>$

$e^{-\frac{i2\pi s(0)}{r}} \qquad e^{-\frac{i2\pi s(1)}{r}} \qquad e^{-\frac{i2\pi s(2)}{r}} \qquad\qquad e^{-\frac{i2\pi s(r-1)}{r}}$

$$|\gamma_s> = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{i2\pi s(k)}{r}} \ |a^k \ mod \ N>$$

Modulare Multiplikation

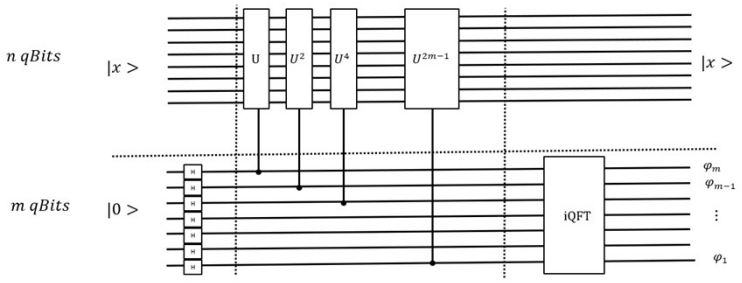
$$U|\gamma_s> = e^{\frac{i2\pi s}{r}} \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{i2\pi s(k)}{r}} \quad |a^k \bmod N> = e^{\frac{i2\pi s}{r}}|\gamma_s>$$

γ_s ist ein Eigenvektor von U mit Eigenwert $e^{\frac{i2\pi s}{r}}$

$U\,|x> = \lambda\,|x>$ $\qquad\qquad$ $\lambda = e^{2\pi i\,\varphi}$

$U^k\,|x> = \lambda^k\,|x> = e^{2\pi i\,k\varphi}\,|x>$

QPE



$$|{+}{+}{+}\cdots{+}>\,|x>$$

$$\underbrace{\frac{1}{\sqrt{2^m}}(|0> + e^{2\pi i\,0.\varphi_1\ldots\varphi_m}\,|1>)\otimes(|0> + e^{2\pi i\,0.\varphi_2\ldots\varphi_m}\,|1>)\ldots\otimes(|0> + e^{2\pi i\,0.\varphi_m}\,|1>)\otimes|x>}$$

$$QFT\,|\varphi_1\ldots\varphi_m>$$

$$|\varphi_1\ldots\varphi_m>\,|x>$$

$$\varphi = \frac{\varphi_1}{2} + \frac{\varphi_2}{4} + \cdots + \frac{\varphi_m}{2^m}$$

QPE

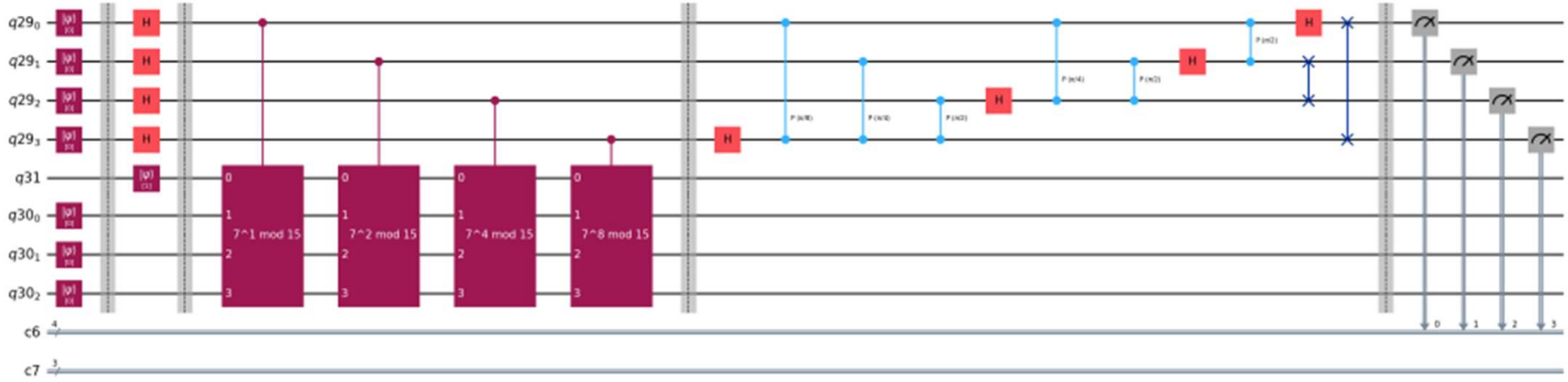
geeignete unitäre Operation U

$$Eigenvektor\ \gamma_s$$

$$\varphi = \frac{s}{r}$$

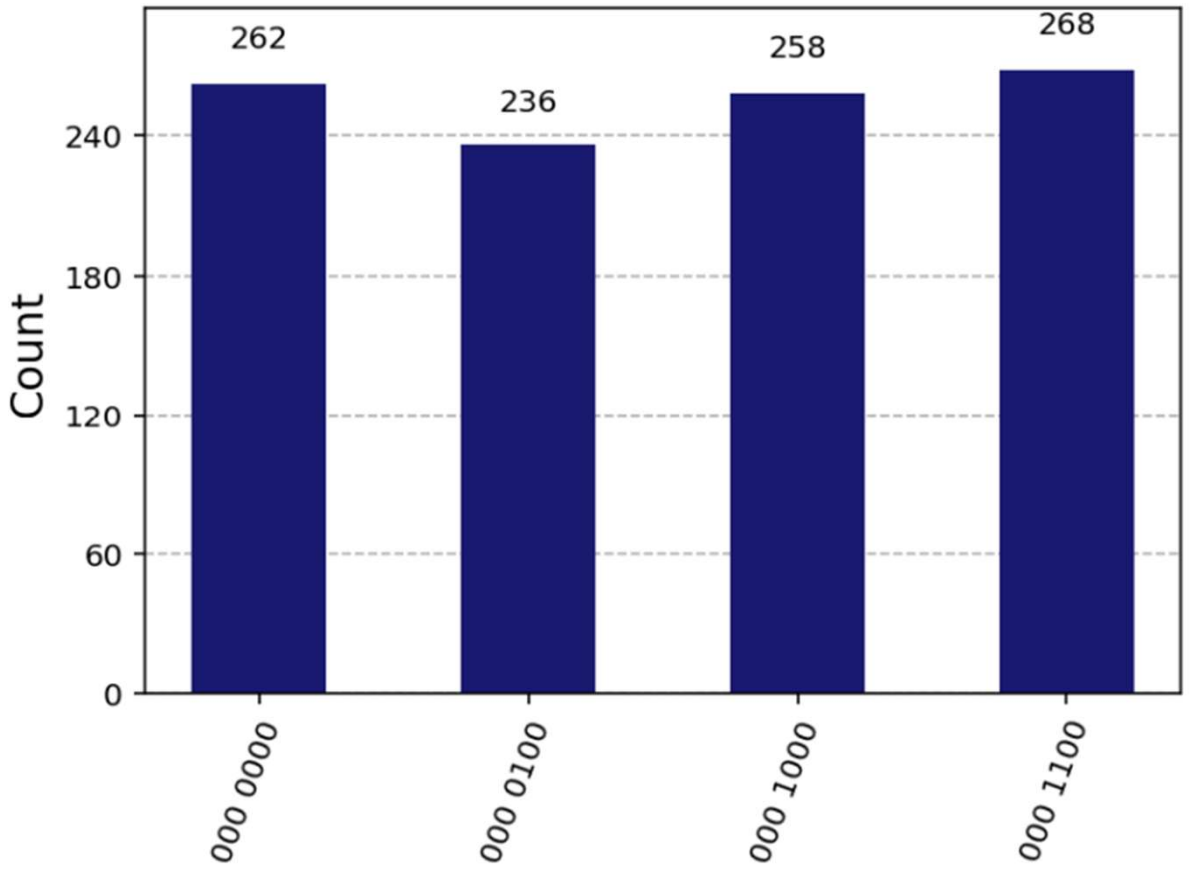
Shor 15

n=15
nx=4
ny=3
a=7



Shor 15

n=15
nx=4
ny=3
a=7



Shor 15

n=15
nx=4
ny=3
a=7

Do Post Processing
Calculate Phases of result

	Register Output	Phase
0	000 0100(bin) = 4(dec)	4/16 = 0.25
1	000 1100(bin) = 12(dec)	12/16 = 0.75
2	000 1000(bin) = 8(dec)	8/16 = 0.50
3	000 0000(bin) = 0(dec)	0/16 = 0.00

---

continued fraction algorithm

	Phase	Fraction	Guess for r
0	0.25	1/4	4
1	0.75	3/4	4
2	0.50	1/2	2
3	0.00	0/1	1

---

calculate the guesses
Potentieller FaktorI 3.0
Potentieller FaktorII 5.0

Potentieller FaktorI 3.0
Potentieller FaktorII 5.0

Potentieller FaktorI 3.0
Potentieller FaktorII 1.0
