

Periodenbestimmung der Funktion $k \rightarrow a^k \bmod N$ mittels Fouriertransformation
Anwendung auf die Faktorisierung ganzer Zahlen (Shors Algorithmus)

```
> with(numtheory):
```

```
Warning, the protected name order has been redefined and unprotected
```

```
> omegalist := proc (m)
```

```
#  
# Numerische Berechnung der komplexen m-ten Einheitswurzeln  
#  
local omega;  
option remember;  
omega := exp(2*Pi*I/m);  
[seq(evalf(omega^k),k=0..m-1)];  
end:
```

```
> omegalist(16);
```

```
[1., 0.9238795325 + 0.3826834325 I, 0.7071067811 + 0.7071067814 I, 0.3826834321 + 0.9238795328 I,  
-5.159051076 10-10 + 1.000000000 I, -0.3826834330 + 0.9238795325 I,  
-0.7071067819 + 0.7071067808 I, -0.9238795331 + 0.3826834316 I,  
-1.000000000 - 1.031810215 10-9 I, -0.9238795324 - 0.3826834336 I, -0.7071067806 - 0.7071067824 I,  
-0.3826834312 - 0.9238795335 I, 1.547715323 10-9 - 1.000000000 I, 0.3826834341 - 0.9238795324 I,  
0.7071067829 - 0.7071067803 I,  
0.9238795338 - 0.3826834308 I]
```

```
> period := proc(N,m,a,p)
```

```
#  
# N : die zu faktorisierende Zahl für den Shor-Algorithmus  
# m : Potenz von 2 für Fourier-Transformation (es sollte  $N^2 < m < 2 N^2$   
# sein)  
# a : Element von  $\mathbb{Z}_N$ , dessen Ordnung mod N  
# (= Periodenlänge der Funktion  $k \rightarrow a^k \bmod N$ )  
# bestimmt werden soll  
# p : Periode in der Fourier-Transformierten  
#  
# liefert die Wahrscheinlichkeit, dass Periode p gemessen wird  
#  
local ol;  
ol := omegalist(m);  
norm(map(evalf,collect(add(ol[p*k mod m + 1]*X^(a^k mod  
N),k=0..m-1),X)),2)^2/m^2;  
end:
```

```
> testperiod := proc (N,m,a)
```

```
#  
# Summe der Wahrscheinlichkeiten  
#  
add(period(N,m,a,p),p=0..m-1)  
end:
```

```
> testperiod(17,32,5);
```

```
1.000000000
```

```
> display_period := proc(N,m,a)
```

```
#
```

```
# Spektrogramm der Periodenmessung für k -> a^k mod N
```

```
#
```

```
[seq([p,period(N,m,a,p)],p=0..m-1)];
```

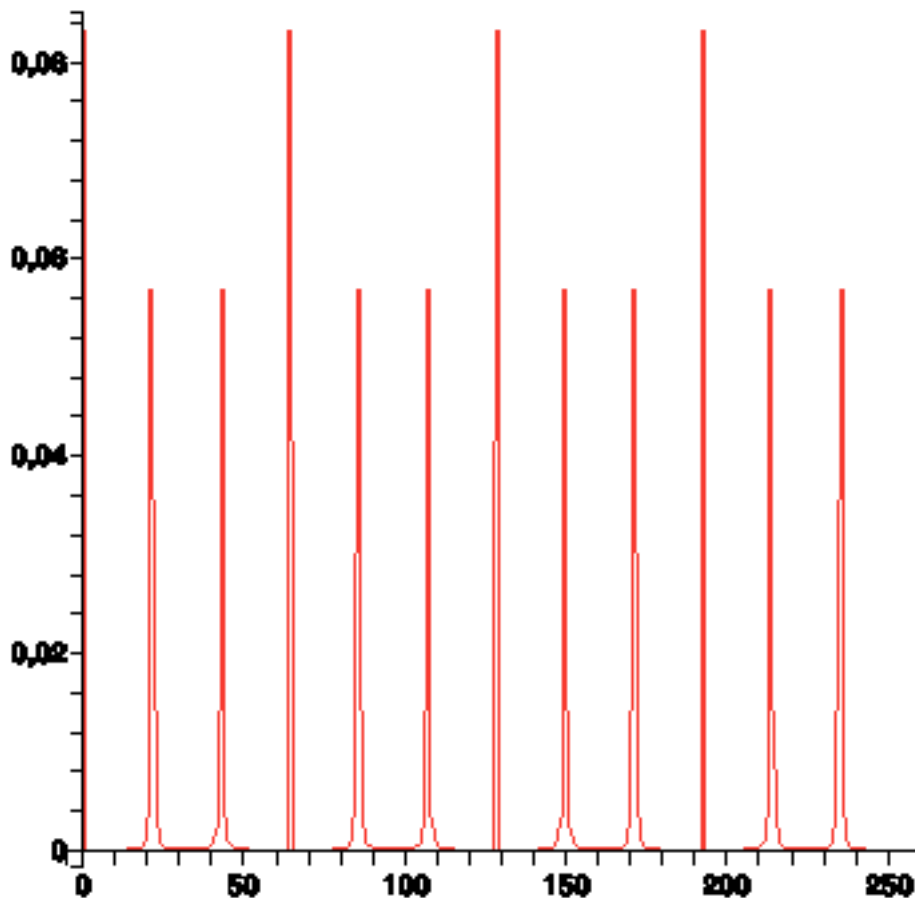
```
plot(%);
```

```
end;
```

Faktorisierung von $N=35$

Daten: $a=2$, $m=256$

```
> display_period(35,256,2);
```



Beispiele für Messwerte: $y = 107, 159, 192, 213$

```
> convert(107/256,confrac,'cvgts');
```

```
[0, 2, 2, 1, 1, 4, 1, 3]
```

```
> cvgts;
```

$$\left[0, \frac{1}{2}, \frac{2}{5}, \frac{3}{7}, \frac{5}{12}, \frac{23}{55}, \frac{28}{67}, \frac{107}{256} \right]$$

```
> convert(159/256,confrac,'cvgts');
```

```
[0, 1, 1, 1, 1, 1, 3, 2, 1, 2]
```

```
> cvgts;
```

$$\left[0, 1, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \frac{18}{29}, \frac{41}{66}, \frac{59}{95}, \frac{159}{256} \right]$$

```
> convert(192/256,confrac,'cvgts');
```

```
[0, 1, 3]
```

```
> cvgts;
```

$$\left[0, 1, \frac{3}{4} \right]$$

```
> convert(213/256,confrac,'cvgts');
```

```
[0, 1, 4, 1, 20, 2]
```

```
> cvgts;
```

$$\left[0, 1, \frac{4}{5}, \frac{5}{6}, \frac{104}{125}, \frac{213}{256} \right]$$

```
> order(2,35);
```

```
12
```

```
> A := 2^(6) mod 35;
```

```
A := 29
```

```
> gcd(A+1,35);
```

```
5
```

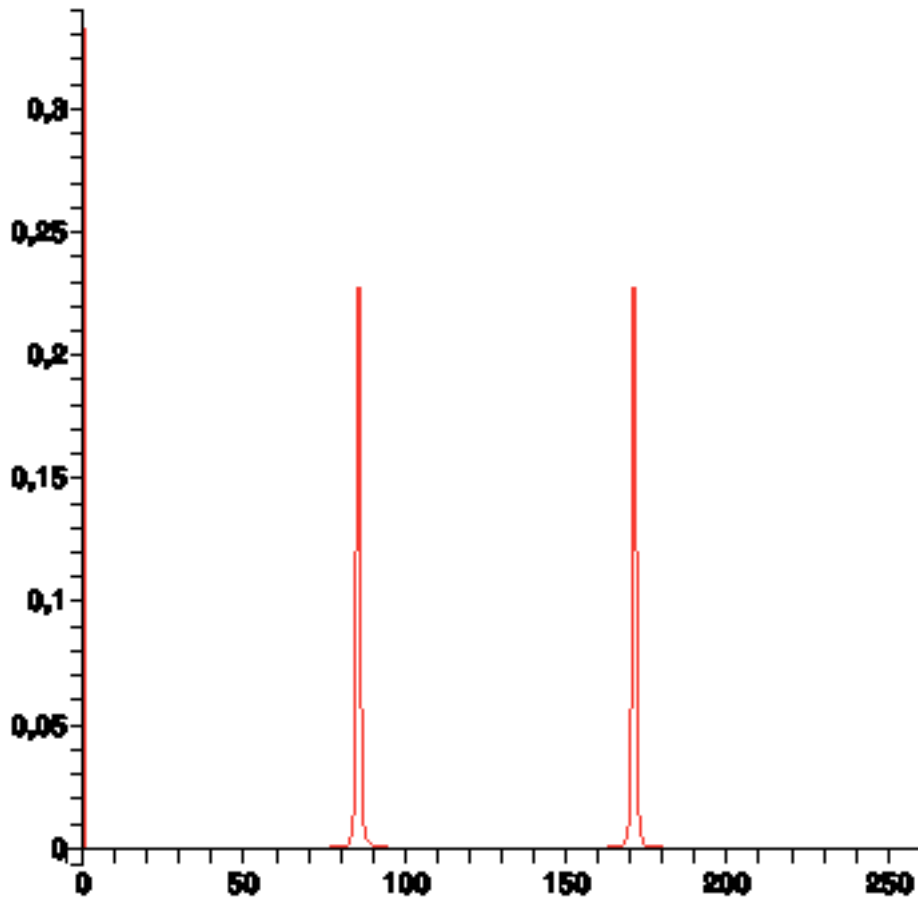
```
> gcd(A-1,35);
```

```
7
```

```
Faktorisierung von N=35
```

```
Daten: a=11, m=256
```

```
> display_period(35,256,11);
```



Mögliche Messwerte: $y = 85, 171$

```
> convert(85/256,confrac,'cvgts');
[0, 3, 85]
```

```
> cvgts;
[ 0, 1/3, 85/256]
```

```
> convert(171/256,confrac,'cvgts');
[0, 1, 2, 85]
```

```
> cvgts;
[ 0, 1, 2/3, 171/256]
```

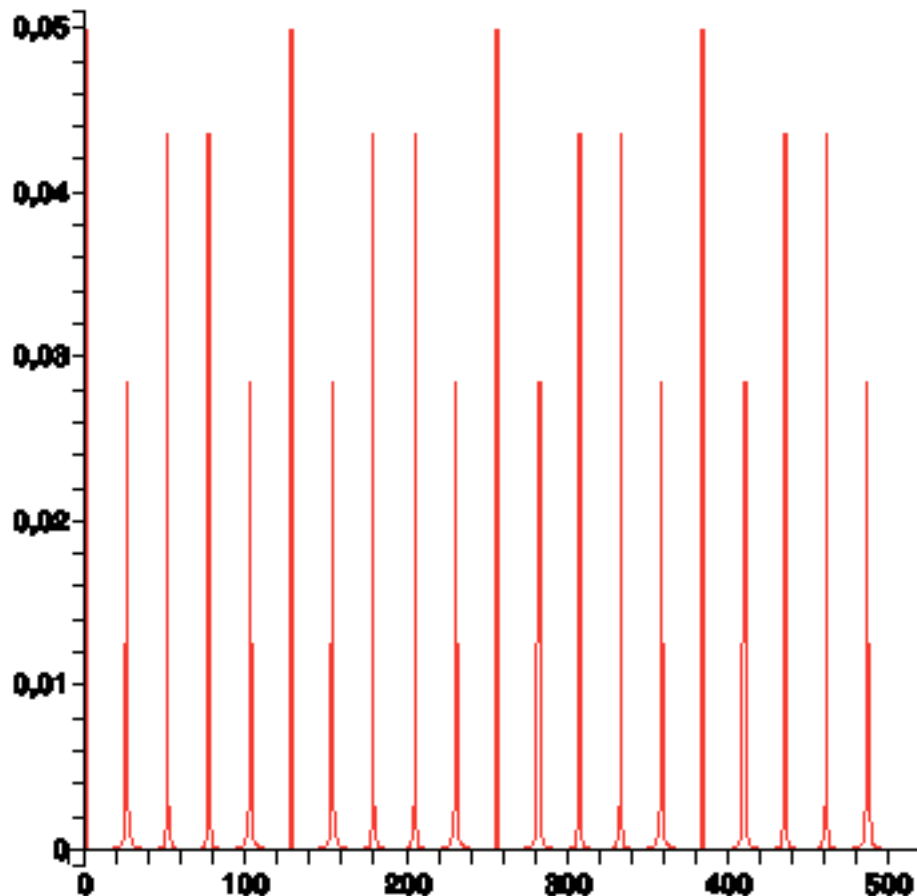
```
> order(11,35);
3
```

Dieser Wert ist für die Faktorisierung nicht brauchbar!

Faktorisierung von N=55

Daten : a=3, m=512

```
> display_period(55,512,3);
```



Beispiele für Messwerte: y = 179, 410, 333, 359

```
> convert(179/512,confrac,'cvgts');
```

```
[0, 2, 1, 6, 6, 4]
```

```
> cvgts;
```

```
[ 0,  $\frac{1}{2}$ ,  $\frac{1}{3}$ ,  $\frac{7}{20}$ ,  $\frac{43}{123}$ ,  $\frac{179}{512}$  ]
```

```
> convert(410/512,confrac,'cvgts');
```

```
[0, 1, 4, 51]
```

```
> cvgts;
```

$$\left[0, 1, \frac{4}{5}, \frac{205}{256} \right]$$

```
> convert(333/512,confrac,'cvgts');
```

```
[0, 1, 1, 1, 6, 6, 4]
```

```
> cvgts;
```

$$\left[0, 1, \frac{1}{2}, \frac{2}{3}, \frac{13}{20}, \frac{80}{123}, \frac{333}{512} \right]$$

```
> convert(358/512,confrac,'cvgts');
```

```
[0, 1, 2, 3, 12, 2]
```

```
> cvgts;
```

$$\left[0, 1, \frac{2}{3}, \frac{7}{10}, \frac{86}{123}, \frac{179}{256} \right]$$

```
> order(3,55);
```

```
20
```

```
> A := 3^10 mod 55;
```

```
A := 34
```

```
> gcd(A+1,55);
```

```
5
```

```
> gcd(A-1,55);
```

```
11
```

```
>
```