

```

In[20]:= NN = 1241143;
         k = 8 × 9 × 5 × 7 × 11 × 13
Out[21]= 360360

In[22]:= Mod[2k - 1, NN]
Out[22]= 861525

In[23]:= GCD[Mod[2k - 1, NN], NN]
Out[23]= 547

In[24]:= FactorInteger[NN]
Out[24]= {{547, 1}, {2269, 1}}

In[25]:= FactorInteger[546]
Out[25]= {{2, 1}, {3, 1}, {7, 1}, {13, 1}}

In[121]:= l = 100;
          p = RandomPrime[{2l, 2l+1}]
          q = RandomPrime[{2l, 2l+1}]
          NN = p q
          FactorInteger[p - 1]
          FactorInteger[q - 1]
Out[124]= 3658257361478318230350717195121690412201036551628760139948459

Out[125]= {{2, 4}, {3, 1}, {7, 1}, {23, 1}, {37, 1},
          {47, 1}, {83, 1}, {1844791708796414711521, 1}}

Out[126]= {{2, 1}, {3, 4}, {397, 1}, {443, 1}, {16123099, 1}, {19990561, 1}, {193597337, 1}}

In[34]:= k = 8 × 9 × 5 × 7 × 11;
          GCD[Mod[2k - 1, NN], NN]
          p
          q
Out[35]= 199
Out[36]= 199
Out[37]= 131

In[127]:= L[n_, u_, v_] := Exp[v Log[n]u Log[Log[n]]1-u]

In[131]:= L[nn, 0, v]
Out[131]= Log[nn]v

In[132]:= L[nn, 1, v]
Out[132]= nnv

```

Quadratic Sieve

```
In[136]:= QS[n_] := L[n,  $\frac{1}{2}$ , 1]
```

Number Field Sieve (NFS/GNFS)

```
In[135]:= NFS[n_] := L[n,  $\frac{1}{3}$ ,  $\left(\frac{64}{9}\right)^{\frac{1}{3}}$ ]
```

```
In[146]:= DiscretePlot[NFS[ $10^n$ ]/QS[ $10^n$ ], {n, 10, 200}] // N // MatrixForm
```

Out[146]//MatrixForm=

