The Universal Exponent Factoring Method

This notebook shows how we can factor n if we know e and d.

```
n:=211463707796206571; e:=9007
```

211463707796206571

9007

```
d:=116402471153538991
```

116402471153538991

Then raising anything to the power r=e*d-1 gives 1.

```
r:=e*d-1
```

104843705767992569 1936

```
powermod(2,r,n)
```

1

We start by pulling out powers of 2 from r.

```
r1:=r/4
```

26210926441998142 2984

```
r2:=r1/4
```

6552731610499535 5746

```
r3:=r2/2
```

32763658052497677873

```
powermod(2,r3,n)
```

187568564780117371

This is not 1. So we work our way up, one factor of 2 at a time.

```
a:=powermod(2,r2,n)
```

113493629663725812

```
powermod(2,2*r2,n)
```

1

OK, we're in business, because a=2^(r2) is neither 1 nor -1 mod n, but 2^(2*r2) is 1. In other words, a is a non-trivial square root of 1. That means a^2=(a+1)(a-1) is divisible by n.

```
gcd(n,a-1)
```

```
gcd(n,a-1)
```

```
885320963
```

```
n/%
```

```
238855417
```

Check:

```
ifactor(n)
```

```
238855417 885320963
```