

```
1 + 1
```

```
2
```

```
n = 12007001
```

```
12007001
```

```
<< "NumberTheory`ContinuedFractions`"
```

In the program below we compute the values $(-1)^{(k+1)} * q[k+1]$ that satisfy $num[k]^2 = (-1)^{(k+1)} * q[k+1] \pmod{n}$, where $num[k]$ is the numerator of the k -th convergent of $\text{Sqrt}[n]$ obtained from the continued fraction expansion of $\text{Sqrt}[n]$.

NOTE: $num[k]$ is NOT equal to $p[k]$ in the algorithm below. We have to get $num[k]$ using the `Convergents` command in Mathematica.

```
p[0] = 0; q[0] = 1; a[0] = Floor[Sqrt[n]]; p[1] = a[0]; q[1] = n - p[1]^2
```

```
776
```

```
FactorInteger[q[1]]
```

```
{{2, 3}, {97, 1}}
```

$-q[1]$ is a square (mod n).

```
Convergents[Sqrt[n], 1]
```

```
{3465}
```

So $(num[1])^2 = 3465^2 = -q[1] \pmod{n}$.

The following program computes the values $(-1)^{(k+1)} q[k+1]$. We'll do it for k up to 20 to see what we can conclude.

```

Do[a[k] = Floor[(p[k] + a[0]) / q[k]];
  p[k + 1] = a[k] * q[k] - p[k]; q[k + 1] = (n - p[k + 1]^2) / q[k];
  Print[(-1)^(k + 1) "q"[k + 1], " ", "=", " ", (-1)^(k + 1) * q[k + 1],
    " ", "=", " ", (-1)^(k + 1), " ", FactorInteger[q[k + 1]]], {k, 1, 20}]

q[2] = 5777 = 1 {{53, 1}, {109, 1}}
-q[3] = -485 = -1 {{5, 1}, {97, 1}}
q[4] = 2696 = 1 {{2, 3}, {337, 1}}
-q[5] = -2785 = -1 {{5, 1}, {557, 1}}
q[6] = 40 = 1 {{2, 3}, {5, 1}}
-q[7] = -5881 = -1 {{5881, 1}}
q[8] = 1021 = 1 {{1021, 1}}
-q[9] = -4856 = -1 {{2, 3}, {607, 1}}
q[10] = 1475 = 1 {{5, 2}, {59, 1}}
-q[11] = -4787 = -1 {{4787, 1}}
q[12] = 1136 = 1 {{2, 4}, {71, 1}}
-q[13] = -2017 = -1 {{2017, 1}}
q[14] = 1685 = 1 {{5, 1}, {337, 1}}
-q[15] = -4456 = -1 {{2, 3}, {557, 1}}
q[16] = 1471 = 1 {{1471, 1}}
-q[17] = -5227 = -1 {{5227, 1}}
q[18] = 400 = 1 {{2, 4}, {5, 2}}
-q[19] = -3595 = -1 {{5, 1}, {719, 1}}
q[20] = 3307 = 1 {{3307, 1}}
-q[21] = -976 = -1 {{2, 4}, {61, 1}}

```

Looking for perfect squares we see that q[18] is a perfect square. We calculate the convergents and we want the numerator of the eighteenth element in the list below :

Convergents[Sqrt[n], 18]

$$\left\{ 3465, \frac{27721}{8}, \frac{31186}{9}, \frac{433139}{125}, \frac{897464}{259}, \frac{2228067}{643}, \frac{384124988}{110855}, \frac{386353055}{111498}, \right.$$

$$\frac{2315890263}{668345}, \frac{2702243318}{779843}, \frac{10422620217}{3007874}, \frac{13124863535}{3787717}, \frac{76046937892}{21946459},$$

$$\left. \frac{241265677211}{69627094}, \frac{799843969525}{230827741}, \frac{1041109646736}{300454835}, \frac{3923172909733}{1132192246}, \frac{4964282556469}{1432647081} \right\}$$

We check that the square of this element (mod n) is the square we got in q[18].

```
PowerMod[4964282556469, 2, n]
```

```
400
```

It is, so to see if I get a nontrivial factor of n from it I calculate :

```
GCD[4964282556469 + 20, n]
```

```
1
```

Unfortunately it does NOT give us a factor. We can compute more convergents to try to find another square, however the next one does not happen until $q[68]$. It DOES give a non-trivial solution, but we will illustrate Method Two for finding values a and c with $a^2 = c^2 \pmod{n}$. We need the values of $q[k]$ up to $q[41]$.

```

Do[a[k] = Floor[(p[k] + a[0]) / q[k]];
  p[k + 1] = a[k] * q[k] - p[k]; q[k + 1] = (n - p[k + 1]^2) / q[k];
  Print[(-1)^(k + 1) "q"[k + 1], " ", "=", " ", (-1)^(k + 1) * q[k + 1],
    " ", "=", " ", (-1)^(k + 1), " ", FactorInteger[q[k + 1]]], {k, 21, 40}]

```

```
q[22] = 3727 = 1 {{3727, 1}}
```

```
-q[23] = -3035 = -1 {{5, 1}, {607, 1}}
```

```
q[24] = 2360 = 1 {{2, 3}, {5, 1}, {59, 1}}
```

```
-q[25] = -2399 = -1 {{2399, 1}}
```

```
q[26] = 2840 = 1 {{2, 3}, {5, 1}, {71, 1}}
```

```
-q[27] = -155 = -1 {{5, 1}, {31, 1}}
```

```
q[28] = 2048 = 1 {{2, 11}}
```

```
-q[29] = -2237 = -1 {{2237, 1}}
```

```
q[30] = 4000 = 1 {{2, 5}, {5, 3}}
```

```
-q[31] = -1735 = -1 {{5, 1}, {347, 1}}
```

```
q[32] = 1891 = 1 {{31, 1}, {61, 1}}
```

```
-q[33] = -2440 = -1 {{2, 3}, {5, 1}, {61, 1}}
```

```
q[34] = 3007 = 1 {{31, 1}, {97, 1}}
```

```
-q[35] = -3755 = -1 {{5, 1}, {751, 1}}
```

```
q[36] = 944 = 1 {{2, 4}, {59, 1}}
```

```
-q[37] = -4679 = -1 {{4679, 1}}
```

```
q[38] = 1775 = 1 {{5, 2}, {71, 1}}
```

```
-q[39] = -248 = -1 {{2, 3}, {31, 1}}
```

```
q[40] = 4637 = 1 {{4637, 1}}
```

```
-q[41] = -2201 = -1 {{31, 1}, {71, 1}}
```

Now we note that the factors

-1, 2, 31, 71, 97

come up quite a bit, so we look only at q[k] ' s having only these factors. We get q[1], q[12], q[28], q[34], and q[41] have only those factors. The product of all of these is a square, namely $(-2^9 * 39 * 71)^2 = c^2$. To get a with $a^2 = c^2 \pmod{n}$

We need the numerators of the convergents num[1],

num[12], num[28], num[34], num[41].

Convergents[Sqrt[n], 1]

{3465}

num[1] = 3465

3465

Convergents[Sqrt[n], 12]

$$\left\{ 3465, \frac{27721}{8}, \frac{31186}{9}, \frac{433139}{125}, \frac{897464}{259}, \frac{2228067}{643}, \frac{384124988}{110855}, \frac{386353055}{111498}, \frac{2315890263}{668345}, \frac{2702243318}{779843}, \frac{10422620217}{3007874}, \frac{13124863535}{3787717} \right\}$$

num[12] = 13124863535

13124863535

Convergents[Sqrt[n], 28]

$$\left\{ 3465, \frac{27721}{8}, \frac{31186}{9}, \frac{433139}{125}, \frac{897464}{259}, \frac{2228067}{643}, \frac{384124988}{110855}, \frac{386353055}{111498}, \frac{2315890263}{668345}, \frac{2702243318}{779843}, \frac{10422620217}{3007874}, \frac{13124863535}{3787717}, \frac{76046937892}{21946459}, \frac{241265677211}{69627094}, \frac{799843969525}{230827741}, \frac{1041109646736}{300454835}, \frac{3923172909733}{1132192246}, \frac{4964282556469}{1432647081}, \frac{83351693813237}{24054545542}, \frac{88315976369706}{25487192623}, \frac{171667670182943}{49541738165}, \frac{1118321997467364}{322737621613}, \frac{1289989667650307}{372279359778}, \frac{2408311665117671}{695016981391}, \frac{6106612997885649}{1762313322560}, \frac{14621537660888969}{4219643626511}, \frac{35349688319663587}{10201600575582}, \frac{1570007823726086797}{453090068952119} \right\}$$

num[28] = 1570007823726086797

1570007823726086797

Convergents[Sqrt[n], 34]

$$\left\{ 3465, \frac{27721}{8}, \frac{31186}{9}, \frac{433139}{125}, \frac{897464}{259}, \frac{2228067}{643}, \frac{384124988}{110855}, \frac{386353055}{111498}, \frac{2315890263}{668345}, \frac{2702243318}{779843}, \frac{10422620217}{3007874}, \frac{13124863535}{3787717}, \frac{76046937892}{21946459}, \frac{241265677211}{69627094}, \frac{799843969525}{230827741}, \frac{1041109646736}{300454835}, \frac{3923172909733}{1132192246}, \frac{4964282556469}{1432647081}, \frac{83351693813237}{24054545542}, \frac{88315976369706}{25487192623}, \frac{171667670182943}{49541738165}, \frac{1118321997467364}{322737621613}, \frac{1289989667650307}{372279359778}, \frac{2408311665117671}{695016981391}, \frac{6106612997885649}{1762313322560}, \frac{14621537660888969}{4219643626511}, \frac{35349688319663587}{10201600575582}, \frac{1570007823726086797}{453090068952119}, \frac{4745373159497923978}{1369471807431939}, \frac{11060754142721934753}{3192033683815997}, \frac{15806127302219858731}{4561505491247936}, \frac{58479136049381510946}{16876550157559805}, \frac{191243535450364391569}{55191155963927351}, \frac{440966206950110294084}{127258862085414507} \right\}$$

num[34] = 440966206950110294084

440966206950110294084

Convergents[Sqrt[n], 41]

$$\left\{ 3465, \frac{27721}{8}, \frac{31186}{9}, \frac{433139}{125}, \frac{897464}{259}, \frac{2228067}{643}, \frac{384124988}{110855}, \frac{386353055}{111498}, \right.$$

$$\frac{2315890263}{668345}, \frac{2702243318}{779843}, \frac{10422620217}{3007874}, \frac{13124863535}{3787717}, \frac{76046937892}{21946459},$$

$$\frac{241265677211}{69627094}, \frac{799843969525}{230827741}, \frac{1041109646736}{300454835}, \frac{3923172909733}{1132192246}, \frac{4964282556469}{1432647081},$$

$$\frac{83351693813237}{24054545542}, \frac{88315976369706}{25487192623}, \frac{171667670182943}{49541738165}, \frac{1118321997467364}{322737621613},$$

$$\frac{1289989667650307}{372279359778}, \frac{2408311665117671}{695016981391}, \frac{6106612997885649}{1762313322560}, \frac{14621537660888969}{4219643626511},$$

$$\frac{35349688319663587}{10201600575582}, \frac{1570007823726086797}{453090068952119}, \frac{4745373159497923978}{1369471807431939},$$

$$\frac{11060754142721934753}{3192033683815997}, \frac{15806127302219858731}{4561505491247936}, \frac{58479136049381510946}{16876550157559805},$$

$$\frac{191243535450364391569}{55191155963927351}, \frac{440966206950110294084}{127258862085414507}, \frac{632209742400474685653}{182450018049341858},$$

$$\frac{1073175949350584979737}{309708880134756365}, \frac{7071265438503984564075}{2040703298857880048}, \frac{8144441387854569543812}{2350412178992636413},$$

$$\frac{31504589602067693195511}{9091939835835789287}, \frac{858768360643682285822609}{247832787746558947162}, \frac{890272950245749979018120}{256924727582394736449} \left. \right\}$$

num[41] = 890272950245749979018120

890272950245749979018120

**We take a = num[1] * num[12] * num[28] * num[34] * num[41] and
c = -2^9 * 31 * 71 * 97 from above.**

a = num[1] * num[12] * num[28] * num[34] * num[41]

28030338292211359167777913063046906774323773951166354853311013162667665244000

c = -2^9 * 31 * 71 * 97

-109310464

GCD[a + c, n]

3001

So we get 3001 is a factor of n.

`n / 3001`

4001

The third method we illustrate is called the Quadratic Sieve Method. Since any QR for n is a QR for any primes dividing n , by determining which primes less than $\text{Sqrt}[n]$ are QR's for the QR's produced in our list we can drastically reduce the set of primes that can possibly divide n .

We will focus on finding on squares less than 100.

By analyzing the above list we see that $q[6]$, $q[10]$, $q[12]$ and $q[21]$ show 10, 59, -61 and 71 are numbers less than 100 that are QRs for n . Since they must be QRs for any prime dividing n we was Mathematica to give us the list of primes less than square root of n that are QR's for these numbers.

We compute square root of n .

`N[Sqrt[n]]`

3465.11

In the command below, `PrimePi` gives the number of primes less than the given number (in this case 3465), since `Prime[k]` gives the k -th prime number, `Prime[Range[2, PrimePi[3465]]]` lists the primes less than 3465.

`Select[Prime[Range[2, PrimePi[3465]]],
Union[JacobiSymbol[{10, 59, -61, 71}, #]] == {1} &]`

{31, 67, 227, 293, 467, 853, 1361, 1427, 1471, 1693, 1733, 1867, 1933, 1987,
2039, 2311, 2441, 2551, 2557, 2591, 2801, 2963, 2969, 3001, 3067, 3079, 3089}

```
PrimePi[3465]
```

```
485
```

There are 485 primes less than 3465. The above left only 27 as possible divisors of n.

This is still quite a few primes, so we consider more squares computed from the continued fraction algorithm.

From line q[28] I get that 2 is a QR. Since 10 was a QR, but $10 = 2 * 5$ this implies 5 is a QR (since $QR * QR = QR$). Then q[27] gives - 31 is a QR and going back to q[3] I get - 97 is a QR. Adding these to my list (and now removing 10, which is unnecessary)

I
get :

```
Select[Prime[Range[2, PrimePi[3465]]],  
Union[JacobiSymbol[{2, 5, -31, 59, -61, 71, -97}, #]] == {1} &]
```

```
{1361, 2551, 2591, 3001}
```

Throwing in that q[4] shows 337 is a QR I get :

```
Select[Prime[Range[2, PrimePi[3465]]],  
Union[JacobiSymbol[{2, 5, -31, 59, -61, 71, -97, 337}, #]] == {1} &]
```

```
{1361, 2551, 3001}
```

Adding from q[31] that - 347 is a QR I get :

```
Select[Prime[Range[2, PrimePi[3465]]],  
Union[JacobiSymbol[{2, 5, -31, 59, -61, 71, -97, 337, -347}, #]] == {1} &]
```

```
{3001}
```

I am left with only one possible prime that can divide n. I see if it does :

```
n / 3001
```

```
4001
```

3001 * 4001

12007001

So indeed n = 3001 * 4001