All competitive modern integer factorization routines (except the elliptic curve method for finding small prime divisors) search for pairs of integers (x, y) such that x^2 *equiv* y^2 mod n.

```
> convert(sqrt(91),confrac,'cv');
> cv;
```

$$[9, 1, 1, 5, 1, 5, 1, 1, 18, 1, 1]$$

$$\left[9, 10, \frac{19}{2}, \frac{105}{11}, \frac{124}{13}, \frac{725}{76}, \frac{849}{89}, \frac{1574}{165}, \frac{29181}{3059}, \frac{30755}{3224}, \frac{59936}{6283}\right]$$

```
> for i from 1 to 11 do
>    c:=cv[i]: a:=numer(c): b:=denom(c):
>    printf("%d^2-91*%d^2 = %d\n",a,b,a^2-91*b^2);
>    od:
9^2-91*1^2 = -10
10^2-91*1^2 = 9
19^2-91*2^2 = -3
105^2-91*11^2 = 14
124^2-91*13^2 = -3
725^2-91*76^2 = 9
849^2-91*89^2 = -10
1574^2-91*165^2 = 1
29181^2-91*3059^2 = -10
30755^2-91*3224^2 = 9
59936^2-91*6283^2 = -3
> x:=10: y:=3:
> p:=gcd(x+y,91); q:=gcd(x-y,91);
```

$$p := 13$$

$$q := 7$$

For larger values of n, it can take a really long time to get a perfect square! But we can put together different pairs until we get a perfect square.

As an illustration of CFRAC, the continued fraction method of integer factorization, we factor the following:

```
> n:=29763067;
```

$$n := 29763067$$

```
> convert(sqrt(3*n),confrac,'cv');
> cv;
```

$$[9449, 3, 2, 1, 2, 50, 1, 63, 1, 1, 12]$$

$$\left[9449, \frac{28348}{3}, \frac{66145}{7}, \frac{94493}{10}, \frac{255131}{27}, \frac{12851043}{1360}, \frac{13106174}{1387}, \frac{838540005}{88741}, \frac{851646179}{90128}, \frac{1690186184}{178869}, \frac{21133880387}{2236556}\right]$$

```
> c:=cv[1]; a1:=numer(c); b1:=denom(c);
> y1:=ifactor(a1^2-3*n*b1^2);
```

$$c := 9449$$

$$a1 := 9449$$

$$b1 := 1$$

$$y1 := -(2)^5\,(5)^2\,(7)$$

```
> convert(sqrt(10*n),confrac,'cv');
> cv;
```

$$[17251, 1, 40, 2, 1, 2, 4, 3, 9, 1, 3]$$

$$\left[17251, 17252, \frac{707331}{41}, \frac{1431914}{83}, \frac{2139245}{124}, \frac{5710404}{331}, \frac{24980861}{1448}, \frac{80652987}{4675}, \frac{750857744}{43523}, \frac{831510731}{48198}, \frac{3245389937}{188117}\right]$$

```
> c:=cv[4]; a2:=numer(c); b2:=denom(c);
> y2:=ifactor(a2^2-10*n*b2^2);
```

$$c := \frac{1431914}{83}$$

$$a2 := 1431914$$

$$b2 := 83$$

$$y2 := (2)\,(3)^3\,(7)\,(47)$$

```
> convert(sqrt(19*n),confrac,'cv');
> cv;
```

$$[23780, 4, 1, 4, 2, 7, 1, 21, 1, 2, 1]$$

$$\left[23780, \frac{95121}{4}, \frac{118901}{5}, \frac{570725}{24}, \frac{1260351}{53}, \frac{9393182}{395}, \frac{10653533}{448}, \frac{233117375}{9803}, \frac{243770908}{10251}, \frac{720659191}{30305}, \frac{964430099}{40556}\right]$$

```
> c:=cv[3]; a3:=numer(c); b3:=denom(c);
> y3:=ifactor(a3^2-19*n*b3^2);
```

$$c := \frac{118901}{5}$$

$$a3 := 118901$$

$$b3 := 5$$

$$y3 := -(2)^6\,(3)\,(47)$$

```
> x:=a1*a2*a3;
```

$$x := 1608749005550786$$

```
> y1*y2*y3;
```

$$(2)^{12}\,(5)^2\,(7)^2\,(3)^4\,(47)^2$$

```
> y:=sqrt(expand(%)); ifactor(%);
```

$$y := 947520$$

$$(2)^6\ (3)^2\ (5)\ (7)\ (47)$$

```
> p:=gcd(x+y,n);
```

$$p := 7901$$

```
> q:=gcd(x-y,n);
```

$$q := 3767$$

```
> p*q;
```

$$29763067$$

```
> isprime(p); isprime(q);
```

true

true

```
> ifactor(n);
```

$$(3767)\ (7901)$$

```
>
```