CFRAC (Continued Fraction) Method of Integer Factorization

All competitive modern algorithms for factoring a large integer n (except the elliptic curve method for finding small prime divisors) search for pairs of integers (x, y) such that $x^2 \equiv y^2 \bmod n$. This common feature of most integer factorization methods is due to Fermat. We demonstrate using a very small example for n; then we move to a somewhat larger example.

Small example: factoring $n = 91$

The 'best' rational approximations $\sqrt{91} \approx \frac{x}{y}$ are the continued fraction convergents:

In[1]:=
```
cv=Convergents[Sqrt[91],20]
```

Out[1]=
$$\left\{9, 10, \frac{19}{2}, \frac{105}{11}, \frac{124}{13}, \frac{725}{76}, \frac{849}{89}, \frac{1574}{165}, \frac{29\,181}{3059}, \frac{30\,755}{3224}, \frac{59\,936}{6283}, \frac{330\,435}{34\,639}, \frac{390\,371}{40\,922}, \frac{2\,282\,290}{239\,249}, \frac{2\,672\,661}{280\,171}, \frac{4\,954\,951}{519\,420}, \frac{91\,861\,779}{9\,629\,731}, \frac{96\,816\,730}{10\,149\,151}, \frac{188\,678\,509}{19\,778\,882}, \frac{1\,040\,209\,275}{109\,043\,561}\right\}$$

Each convergent gives a pair of integers (x, y) with $x^2 - 91\,y^2$ relatively small:

In[2]:=
```
For[i=1, i≤20, i++, cvi=NumeratorDenominator[cv[[i]]]; x=cvi[[1]]; y=cvi[[2]]; smint=x^2-91*y^2;
   Print[x^HoldForm[2]," - 91*",y^HoldForm[2]," = ",smint]]
```

$9^2 - 91*1 = -10$

$10^2 - 91*1 = 9$

$19^2 - 91*2^2 = -3$

$105^2 - 91*11^2 = 14$

$124^2 - 91*13^2 = -3$

$725^2 - 91*76^2 = 9$

$849^2 - 91*89^2 = -10$

$1574^2 - 91*165^2 = 1$

$29\,181^2 - 91*3059^2 = -10$

$30\,755^2 - 91*3224^2 = 9$

$59\,936^2 - 91*6283^2 = -3$

$330\,435^2 - 91*34\,639^2 = 14$

$390\,371^2 - 91*40\,922^2 = -3$

$2\,282\,290^2 - 91*239\,249^2 = 9$

$2\,672\,661^2 - 91*280\,171^2 = -10$

$4\,954\,951^2 - 91*519\,420^2 = 1$

$91\,861\,779^2 - 91*9\,629\,731^2 = -10$

$96\,816\,730^2 - 91*10\,149\,151^2 = 9$

$188\,678\,509^2 - 91*19\,778\,882^2 = -3$

$1\,040\,209\,275^2 - 91*109\,043\,561^2 = 14$

Focus on the second entry $10^2 - 91 \cdot 1^2 = 3^2$, which is a square. This gives $10^2 \equiv 3^2 \bmod 91$, so $(10 + 3)(10 - 3) = 10^2 - 3^2$ is divisible by 91. If we are lucky, $10 + 3$ is divisible by a prime factor of 91, and $10 - 3$ is divisible by a different prime factor of 91. To find the common factors we compute

In[3]:=
```
GCD[10+3,91]
GCD[10-3,91]
```

Out[3]= 13

Out[4]= 7

Jackpot, we have factored 91. If we do not see any squares in the right hand column, maybe we can find two values in this column whose products are squares. For example, multiplying lines 3 and 5 gives a square, which tells us $19^2 \cdot 124^2 \equiv (-3)^2 \bmod 91$, so $(19 \cdot 124 + 3)(19 \cdot 124 - 3)$ is divisible by 91. Check for common factors:

In[5]:=
```
GCD[19*124+3,91]
GCD[19*124-3,91]
```

Out[5]= 7

Out[6]= 13

Fermat's idea of looking for small values of $x^2 - n\,y^2$ whose product is a square, is easiest when n is small. When n is larger, the values of $x^2 - n\,y^2$ are however still typically much smaller than n, so these values are often easy enough to factor; and this information will help us to find products which are squares. Let's demonstrate with another example.

Next example: factoring $n = 29\,763\,067$

Continued fraction convergents for $\sqrt{k\,n}$, in place of $\sqrt{n}$, work just as well for our purpose. Here are a few we found useful:

In[7]:=
```
n=29763067; Print["n = ",n]
cv3=Convergents[Sqrt[3*n],5]; Print["cv3 = ",cv3]
cv10=Convergents[Sqrt[10*n],5]; Print["cv10 = ",cv10]
cv19=Convergents[Sqrt[19*n],5]; Print["cv19 = ",cv19]
```

n = 29 763 067

$$\text{cv3} = \left\{9449, \frac{28\,348}{3}, \frac{66\,145}{7}, \frac{94\,493}{10}, \frac{255\,131}{27}\right\}$$

$$\text{cv10} = \left\{17\,251, 17\,252, \frac{707\,331}{41}, \frac{1\,431\,914}{83}, \frac{2\,139\,245}{124}\right\}$$

$$\text{cv19} = \left\{23\,780, \frac{95\,121}{4}, \frac{118\,901}{5}, \frac{570\,725}{24}, \frac{1\,260\,351}{53}\right\}$$

We highlight one convergent from each of these lists, and print the resulting equation (using a function code snippet, essentially a "lambda expression") and also factor the right hand side into prime factors:

In[11]:=
```
f=(nd=NumeratorDenominator[#1]; x=nd[[1]]; y=nd[[2]]; expn=x^2-#2*n*y^2;
   Print[x^HoldForm[2]," - ",#2,"*n*",y^HoldForm[2]," = ",expn," = ",FactorInteger[expn]])& ;
f[cv3[[1]],3]
f[cv10[[4]],10]
f[cv19[[3]],19]
```

$9449^2 - 3*n*1 = -5600 = \{\{-1, 1\}, \{2, 5\}, \{5, 2\}, \{7, 1\}\}$

$1\,431\,914^2 - 10*n*83^2 = 17\,766 = \{\{2, 1\}, \{3, 3\}, \{7, 1\}, \{47, 1\}\}$

$118\,901^2 - 19*n*5^2 = -9024 = \{\{-1, 1\}, \{2, 6\}, \{3, 1\}, \{47, 1\}\}$

The product on the left hand side is congruent to $(9449 \cdot 1\,431\,914 \cdot 118\,901)^2$ mod n. The product of the right hand sides factors as $(-1)^2 \cdot 2^{12} \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 47^2 = (2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 47)^2$. We have two squares in the same congruence class mod n, so we check

In[23]:=
```
x=9449*1431914*118901; Print["x = ",x]
y=2^6*3^2*5*7*47; Print["y = ",y]
p=GCD[x+y,n]; Print["p = ",p]
q=GCD[x-y,n]; Print["q = ",q]
```

```
x = 1 608 749 005 550 786
y = 947 520
p = 7901
q = 3767
```

Check that p and q are prime, and that their product is n.

In[19]:=
```
PrimeQ[p]
PrimeQ[q]
Print["p*q = ",p*q]
Print["n = ",n]
```

Out[19]=
```
True
```

Out[20]=
```
True
```

```
p*q = 29 763 067
n = 29 763 067
```