

Math 110 In-Class Discussion
April 21, 2005

Here's the computation we did to determine the prime factors of $m = pq$ when p and q are close together.

```
parisize = 4000000, primelimit = 500000
(08:15) gp > nextprime(160000)
%1 = 160001
(08:15) gp > nextprime(170000)
%2 = 170003
(08:16) gp > nextprime(162000)
%3 = 162007
(08:16) gp > 162007*160001
%4 = 25921282007
(08:17) gp > m=%
%5 = 25921282007
(08:17) gp > t=floor(sqrt(m))+1
%6 = 161001
(08:19) gp > sqrt(t^2-m)
%7 = 199.9849994374578085445065450
(08:19) gp > sqrt((t+1)^2-m)
%8 = 601.6618651701302566110415654
(08:19) gp > sqrt((t+2)^2-m)
%9 = 827.0441342516129592285403469
(08:20) gp > sqrt((t+3)^2-m)
%10 = 1003.0000000000000000000000000000
```

So then since $m = pq$ (with say $p > q$) we can write, as done by Fermat,

$$m = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$$

Letting

$$s = \frac{p-q}{2} \quad t = \frac{p+q}{2}$$

we can solve for p and q in terms of s and t giving

$$p = t + s \quad q = t - s$$

Now back to the PARI computation, the t that gives us $\sqrt{t^2 - m}$ an integer is $t = 161004$ and results in an $s = 1003$. Adding and subtracting these recovers p and q .