The Fermat Factorization Method

R. C. Daileda

Trinity University

Number Theory

Introduction

Recall: The security of the RSA cryptosystem depends on the difficulty in factoring the encryption modulus $n = pq$.

Poor choices of p and q can lead to easily factored values of n, rendering the cryptosystem "cracked."

One such situation occurs when p and q are relatively close together. In this case one can apply the *Fermat Factorization Method* to find p and q.

Remark: The Fermat method can be applied to arbitrary odd n to try to find a divisor/complementary divisor pair that are relatively close together, if such a pair exists.

The Set-up

Suppose that $n = ab$ with $a > b$ odd. Notice that

$$\begin{aligned} n &= ab \\ &= \left(\frac{a+b}{2} + \frac{a-b}{2}\right)\left(\frac{a+b}{2} - \frac{a-b}{2}\right) \\ &= \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2. \end{aligned}$$

If a and b are close together, then:

- $\dfrac{a-b}{2}$ is relatively small; specifically we assume $\dfrac{a-b}{2\sqrt{2b}} < \epsilon$.
- $\dfrac{a+b}{2}$ is not much larger than $\sqrt{n}$.

To quantify this final statement note that

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \;\Rightarrow\; \left(\frac{a+b}{2}\right)^2 - n = \left(\frac{a-b}{2}\right)^2$$

and hence

$$\left(\frac{a+b}{2} - \sqrt{n}\right)\left(\frac{a+b}{2} + \sqrt{n}\right) = \left(\frac{a-b}{2}\right)^2.$$

Since

$$\left(\frac{a+b}{2} + \sqrt{n}\right) > 2b \quad \text{and} \quad \left(\frac{a-b}{2}\right)^2 > 0$$

we obtain

$$0 < \frac{a+b}{2} - \sqrt{n} < \left(\frac{a-b}{2\sqrt{2b}}\right)^2 < \epsilon^2.$$

The Algorithm: Fermat Factorization

Moral: If n is the product of two distinct odd numbers that are close together, then

$$n = t^2 - s^2$$

where t is slightly larger than $\sqrt{n}$ and s is relatively small.

How can we use this to factor n? Set $t_0 = \lceil \sqrt{n} \rceil$ and successively compute

$$\sqrt{t_0^2 - n}, \sqrt{(t_0+1)^2 - n}, \sqrt{(t_0+2)^2 - n}, \sqrt{(t_0+3)^2 - n}, \ldots$$

until one obtains

$$\sqrt{(t_0+k)^2 - n} = s \in \mathbb{N}.$$

If we set $t = t_0 + k$, then $n = t^2 - s^2 = (t+s)(t-s)$.

Remarks:

- Because of our assumption on $(a-b)/2$, this process is guaranteed to stop after roughly ϵ^2 steps.
- The factors $(t+s)$ and $(t-s)$ are nontrivial because $t \sim \sqrt{n}$ while $s \sim 0$.

Example

Apply the Fermat Factorization Method to factor

$$n = 2251644881930449333.$$

We have

$$t_0 = \lceil \sqrt{n} \rceil = 1500548194.$$

Moreover, we find that

$$\begin{aligned}
\sqrt{t_0^2 - n} &= \sqrt{586212303} = 24211.821\ldots,\\
\sqrt{(t_0+1)^2 - n} &= 2\sqrt{896827173} = 59894.145\ldots,\\
\sqrt{(t_0+2)^2 - n} &= \sqrt{6588405083} = 81168.990\ldots,\\
\sqrt{(t_0+3)^2 - n} &= 97926
\end{aligned}$$

so that $t = t_0 + 3 = 1500548197$ and $s = 97926$.

Hence $n = pq$ with

$$\begin{aligned}
p &= t + s = 1500646123,\\
q &= t - s = 1500450271,
\end{aligned}$$

both of which turn out to be prime. Note $\left(\dfrac{p-q}{2\sqrt{2q}}\right)^2 = 3.1955\ldots$.

Example

The integer

$$n = 8956494142912946049415883818712449246261041215620422273183844943817234975145408604748034940414 79529$$

is the product of two primes. Use Fermat Factorization to find them.

We have

$$t_0 = \lceil\sqrt{n}\rceil = 299274023979912864896278711430112859377494363822 09$$

and with the aid of a computer we find that

$$\sqrt{(t_0+18)^2-n} = 33408832099552561140000000.$$

Hence

$$s = 33408832099552561140000000,$$
$$t = 29927402397991286489627871143011285937749436382227,$$

so that the prime factorization of n is pq where

$$p = 29927402397991286489627837734179186385188296382227,$$
$$q = 29927402397991286489627904551843385490310576382227.$$

Note that $\left(\dfrac{p-q}{2\sqrt{2p}}\right)^2 = 18.6476\ldots.$

Remark: Factoring n in this manner only took a matter of minutes using Maple. However, after over 8 hours neither Maple nor PARI could successfully factor n naïvely.