Wiener Attack Handout

Matt Cheung

July 24, 2017

First step is to approximate $\frac{e}{pq}$ using continued fractions of the form

$$\cfrac{a_1}{q_1 + \cfrac{a_2}{q_2 + \cfrac{a_3}{\cfrac{\cdots}{q_{m-1} + \cfrac{a_m}{q_m}}}}}$$

with all $a_i = 1$.

1 Continued Fraction Expansion

Continued fraction expansion of a fraction f.

$$\begin{array}{lll} q_0 = \lfloor f \rfloor & r_0 = f - q_0 & \\ q_i = \lfloor \frac{1}{r_{i-1}} \rfloor & r_i = \frac{1}{r_i} - q_i & \text{for } i = 1, 2, \cdots, m \end{array}$$

Return $\langle q_0, q_1, \cdots, q_m \rangle$

Example: $\frac{1387}{2719} = \langle 0, 1, 1, 24, 4, 1, 1, 2, 2 \rangle$

2 Reconstructing f From Expansion

$$\begin{array}{lll} n_0 = q_0 & d_0 = 1, & \\ n_1 = q_0 q_1 + 1 & d_1 = q_1, & \\ n_i = q_i n_{i-1} + n_{i-2} & d_i = q_i d_{i-1} + d_{i-2}, & \text{for } i = 2, 3, \cdots, m \end{array}$$

Useful Fact: $n_i d_{i-1} - n_{i-1} d_i = -(-1)^i$ for $i = 1, 2, \cdots, m$.

3 Continued Fraction Algorithm

Let f' be an underestimate of f

$$f' = (1 - \delta) f \text{ for some } \delta > 0$$

In this case $f' = \frac{e}{pq} = \frac{e}{n}$ and $f = \frac{k}{dg}$

Steps of the Algorithm:

- Generate the next quotient (q'_i) for the continued fraction expansion of f'
- Construct the following fraction:

$$\begin{array}{ll} \langle q'_0, q'_1, \cdots, q'_{i-1}, q'_i + 1\rangle & \text{if } i \text{ is even} \\ \langle q'_0, q'_1, \cdots, q'_{i-1}, q'_i\rangle & \text{if } i \text{ is odd} \end{array}$$

- Check if the fraction equals f

An important equation $edg = k(p-1)(q-1) + g$. This allows for guesses for $(p-1)(q-1)$ and g.

Using this guess and $\frac{pq-(p-1)(q-1)+1}{2} = \frac{p+q}{2}$

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

Through an example we will show how to check do the check step.

$$pq = 8927 \qquad \text{and} \qquad e = 2621$$

so $\frac{e}{pq} = \frac{2621}{8927}$

Calculated Quantity	How it is Derived	$i=0$	$i=1$	$i=2$
q_i'	Continued Fraction Expansion	0	3	2
r_i'	Continued Fraction Expansion	$\frac{2621}{8927}$	$\frac{1064}{2621}$	$\frac{493}{1064}$
$\frac{n_i'}{d_i'}$	Reconstruction Algorithm	$\frac{0}{1}$	$\frac{1}{3}$	$\frac{2}{7}$
guess of $\frac{k}{dg}$	$\langle q_0', q_1', \cdots, q_{i-1}', q_i'+1\rangle (i \text{ even})$	$\frac{1}{1}$	$\frac{1}{3}$	$\frac{3}{10}$
	$\langle q_0', q_1', \cdots, q_i'\rangle (i \text{ odd})$			
guess of edg	$e \cdot dg$	2621	7863	26210
guess of $(p-1)(q-1)$	$\lfloor edg/k \rfloor$	2621	7863	8736
guess of g	$edg \bmod k$	0	0	2
guess of $\frac{p+q}{2}$	see above	3153.5 (quit)	532.5 (quit)	96
guess of $\left(\frac{p-q}{2}\right)^2$	see above			$289 = 17^2$
guess of d	dg/g			5