(2)

Given

$n = pq$

where $p, q \in \mathbb{Z}/p\mathbb{Z}$

factorisation of n not given

Show: knowlege of $p, q \Leftrightarrow$ knowlege of $\varphi(n)$

Proof:

From the definition of the totient function, we have:

$$\varphi(n) = (p-1)(q-1) = pq - p - q + 1$$

Since $n = pq$, we can rewrite as:

$$\varphi(n) = n - p - q + 1$$

rewriting for $p+q$ we have

$$p + q = n + 1 - \varphi(n)$$

We therfore have the system:

$$\left| \begin{array}{l} pq = n \\ p + q = n + 1 - \varphi(n) \end{array} \right.$$

$$\left| \begin{array}{l} pq = n \Rightarrow q = \frac{n}{p} \\ p + \frac{n}{p} = n + 1 - \varphi(n) \quad | \times p \end{array} \right.$$

$$p^2 + n = pn + p - \varphi(n)p$$

$$p^2 - p(n + 1 - \varphi(n)) + n = 0$$

Which gives us a quadratic equation which can be easily solved, given that we have n, $\varphi(n)$, to find p. Finding q is trivial afterwards.

Since we have seen that knowledge of $\varphi(n), n$ is equivalent to knowing p, q, we can also say that knowing $p, q \Leftrightarrow$ knowing $\varphi(n)$

(9)

For $627^i \bmod 941$, a pattern emerges, repeating after every $\approx 0.7\times10^6$ elements ($i = 0.7\times10^6$), when the result of the powermod operation is once again the same in the following calculations (we have made a full „cycle")

For a larger prime, $627^i \bmod p$, the pattern starts repeating much sooner, for $p = 65537$, the pattern repeats every $\approx 0.032 \times 10^6$ elements.

When we take a larger p but a smaller base, the reoccurance of the pattern is rarer. Specifically in the case of $7^{i\times1024} \bmod 65537$, the pattern repeats (very closely to) every 65537 elements.