> $n := 3^3 \cdot 5^2 \cdot 23$

$$n := 15525 \tag{1}$$

We choose g = xˆ77 as the generator of G the cyclic group of order 15525 (we know g generates G as 77 has no common factors with 15525)

> $g := x^{77};$

$$g := x^{77} \tag{2}$$

We aim to find the logarithm of h = xˆ372 in G where G is generated by g

Step 1

> $g1 := x^{77 \cdot 5^2 \cdot 23 \mod 27}$

$$g1 := x^{22} \tag{3}$$

> $h1 := x^{372 \cdot 5^2 \cdot 23 \mod 27}$

$$h1 := x^{6} \tag{4}$$

We need to find the log of h1 = xˆ6 in the cyclic group of order 27 generated by g1 = xˆ22. Using the basic Pohling Hellman algorithm for prime powers or otherwise we find that this is 15 which we can see is true as

> $x^{22 \cdot 15 \mod 27}$

$$x^{6} \tag{5}$$

>

So our first congruence is x1 = 15 mod 27

Step 2

> $g2 := x^{77 \cdot 3^3 \cdot 23 \mod 25}$

$$g2 := x^{17} \tag{6}$$

> $h2 := x^{372 \cdot 3^3 \cdot 23 \mod 25}$

$$h2 := x^{12} \tag{7}$$

We need to find the log of h2 = xˆ12 in the cyclic group of order 25 generated by g2 = xˆ17 ; we see that this is 11 as

> $x^{17 \cdot 11 \mod 25}$

$$x^{12} \tag{8}$$

>

Hence the log of h2 mod 25 is 11 giving x2 = 11 mod 25 as our second congruence

Step 3

>

> $g3 := x^{77 \cdot 3^3 \cdot 5^2} \mod 23$

$$g3 := x^{18} \tag{9}$$

> $h3 := x^{372 \cdot 3^3 \cdot 5^2} \mod 23$

$$h3 := x^9 \tag{10}$$

We need to find the log of h3= xˆ9 in the cyclic group of order 23 generated by g2 = xˆ18; we see that this is 12 as

> $x^{18 \cdot 12} \mod 23$

$$x^9 \tag{11}$$

>

Hence the log of h3 mod 23 is 12 giving x3 = 12 mod 23 as our 3rd congruence

Hence we need to find the unique solution to x = 15 mod 27, x = 11 mod 25, x = 12 mod 23. By the Chinese Remainder Theorem or otherwise we find x = 10086 mod 15525.

We claim that the log of xˆ372 in the cyclic group of order 15525 with generator g = xˆ77 is x = 10086. We can see that this is true as

> $77 \cdot 10086 \mod 15525$

$$372 \tag{12}$$

>

>