$\mathit{find\_log} := \boldsymbol{proc}(n, a, m)$
$\boldsymbol{description}$"Find log of a";
$\boldsymbol{for} i \boldsymbol{from} 1 \boldsymbol{to} n$
$\boldsymbol{do}$
$\boldsymbol{if} a \cdot i \quad \boldsymbol{mod}\ n = m$
$\boldsymbol{then}$
$\boldsymbol{return} i;$
$\boldsymbol{fi};$
$\boldsymbol{enddo};$
$\boldsymbol{endproc};$

>

$\mathit{ifactor}(3267)$

$$(3)^3 (11)^2 \tag{1}$$

$n := 3^3 \cdot 11^2;$

$$n := 3267 \tag{2}$$

g = xˆ13, h = xˆ157, n = 3267; ¡g¿ generatees the group of order 3267;
Steps 1:
$g1 := x^{13 \cdot 11^2 \mod 27};$

$$g1 := x^7 \tag{3}$$

$h1 := x^{157 \cdot 11^2 \mod 27};$

$$h1 := x^{16} \tag{4}$$

We need to find the log of h1 = xˆ16 in the cyclic group of order 27 generated by g1 = xˆ7. By trial and error, we get log(h1) = 10

$\mathit{find\_log}(27, 7, 16);$

>

$$10 \tag{5}$$

So our first congruence is x1 = 10 mod 27 — (1)

Step 2:

$g2 := x^{13 \cdot 3^3 \mod 121};$

$$g2 := x^{109} \tag{6}$$

$h2 := x^{157 \cdot 3^3 \mod 121};$

$$h2 := x^4 \tag{7}$$

We need to find the log of h2 = xˆ4 in the cyclic group of order 121 generated by g2 = xˆ109; using the proc find_log above, it is = 118
find_log(121, 4, 109);

$$118 \tag{8}$$

We get our second congruence as: x2 = 118 mod 121 — (2)

Hence we need to find the unique solution to x = 10 mod 27, and x = 118 mod 121 using Chinese Remainder Theorem.

with(*NumberTheory*);

$$[\mathit{AreCoprime}, \mathit{CalkinWilfSequence}, \mathit{CarmichaelLambda}, \mathit{ChineseRemainder}, \mathit{ContinuedFraction}, \mathit{ContinuedFractionPolynomial}, \mathit{CyclotomicPolynomial}, \mathit{Divisors}, \mathit{FactorNormEuclidean}, \mathit{HomogeneousDiophantine}, \mathit{ImaginaryUnit}, \mathit{InhomogeneousDiophantine}, \mathit{IntegralBasis}, \mathit{InverseTotient}, \mathit{IsCyclotomicPolynomial}, \mathit{IsMersenne}, \mathit{IsSquareFree}, \mathit{IthFermat}, \mathit{IthMersenne}, \mathit{JacobiSymbol}, \mathit{JordanTotient}, \mathit{KroneckerSymbol}, \mathit{Landau}, \mathit{LargestNthPower}, \mathit{LegendreSymbol}, \mathit{M\ddot{o}bius}, \mathit{ModExtendedGCD}, \mathit{ModularLog}, \mathit{ModularRoot}, \mathit{ModularSquareRoot}, \mathit{Moebius}, \mathit{MultiplicativeOrder}, \mathit{M\ddot{o}bius}, \mathit{NearestLatticePoint}, \mathit{NextSafePrime}, \mathit{NumberOfIrreduciblePolynomials}, \mathit{NumberOfPrimeFactors}, \Omega, \Phi, \mathit{PrimeCounting}, \mathit{PrimeFactors}, \mathit{PrimitiveRoot}, \mathit{PseudoPrimitiveRoot}, \mathit{QuadraticResidue}, \mathit{Radical}, \mathit{RepeatingDecimal}, \mathit{RootsOfUnity}, \mathit{SimplestRational}, \mathit{SumOfDivisors}, \mathit{SumOfSquares}, \mathit{ThueSolve}, \mathit{Totient}, \lambda, \mu, \phi, \mathrm{pi}, \sigma, \tau, \varphi] \tag{9}$$

ChineseRemainder([10, 118], [27, 121]);

$$118 \tag{10}$$