


$$N = pq$$

$$29083 = 229 \times 127$$


Checking is easy

Factorization is Hard.

2.

$$\text{g.c.d } (a, b) = c$$

$$\text{Let } a = mc \quad b < a. \\ b = nc$$

$$r = a - bq \quad : c \text{ divides } r$$

$$= (m - nq)c$$

$$\begin{array}{r} 3 \\ \hline 24 \overline{) 75} \\ \underline{72} \end{array}$$

$$g_1 = \left[\begin{array}{c} a \\ b \end{array} \right]$$

$$r_1 = a - bq_1$$

$$g_2 = \left[\begin{array}{c} b \\ r_1 \end{array} \right]$$

$$r_2 = b - q_2 r_1$$

$$g_3 = \left[\begin{array}{c} r_1 \\ r_2 \end{array} \right]$$

$$r_3 : \quad g_{n+1} = \frac{r_{n-1}}{r_n}$$

$$r_n = c$$

$$\begin{array}{r} 3 \overline{) 24} (8 \\ \underline{24} \\ \hline \dots \end{array}$$

Period Finding

- 3 -

1. Given N , Choose a random $m < N$ which is coprime with N

2. Powers of m

$$F_N(a) = m^a \pmod{N}$$

The smallest value of a ($= P$)

$$m^P = 1 \pmod{N}.$$

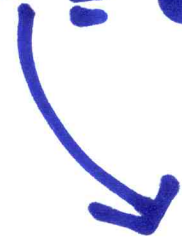
is Period of this function.

$$N = 21.$$

Choose $m = 2$

$$2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32 = 11 \pmod{21}$$

$$2^6 = 64 = 1 \pmod{21}$$



Period.

$$P = 6$$

$$m \in \{2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

$$x^2 = 1 \pmod{N}$$

If N is an odd prime

$$x = \pm 1$$

If N is a composite number

Non-trivial solns

$$x = \pm a \pmod{N}$$

$$x^2 = 1 \pmod{41}$$

$$N = 55 ; \quad x = \pm 21$$

$$\begin{aligned} x^2 = 441 &= 1 \pmod{440} \\ &= 1 \pmod{55} \end{aligned}$$

8 × 55

$$m^p = 1 \pmod{N} \quad x = \cancel{m^{p/2}}$$

6

If p is odd, Algorithm fails

If p is even

$$(m^{p/2} + 1)(\underline{m^{p/2} - 1}) = 0 \pmod{N}.$$

If $m^{p/2} + 1 = kN$ Algorithm fails.

will contain factors of N

$$N = 21 ; m = 2, P = 6.$$

$$(m^{P/2} + 1)(m^{P/2} - 1) = 0 \pmod{N}$$

$$\underbrace{(2^3 + 1)}_{\downarrow 9} \underbrace{(2^3 - 1)}_{\uparrow 7}$$

$$N = 35 ;$$

$$\underline{m = 13}$$

$$13^2 = 169$$

$$13^4 = 28561 = 35 \times 816 + 1$$

$$\underline{P = 4}$$

$$(13^2 + 1)(13^2 - 1)$$

$$= 170 \times 168$$

↑ Factor 5 ↑ Factor 7