THE EUCLIDEAN ALGORITHM

$963 = 657 \times 1 + 306$

$657 = 306 \times 2 + 45$

$306 = 45 \times 6 + 36$

$45 = 36 \times 1 + 9$

$36 = 9 \times 4$

$A = 657$
$B = 963$
$d = (A,B)$

g. c. d.
of A & B

$9 = 45 - 36 = 45 - (306 - 45 \times 6)$

$= -306 + 7 \times 45$

$= -306 + 7(657 - 306 \times 2)$

$= 7 \times 657 - 15 \times 306$

$= 7 \times 657 - 15(963 - 657)$

$= 22 \times 657 - 15 \times 963$

$9 = 22 \times 657 - 15 \times 963$

$d = h\ A + k\ B$

The Euclidean Algorithm

There are integers S and T such that

$$(A, B) = S \cdot A + T \cdot B$$

Example, with

$$A = 247246104 \qquad B = 6402768$$

we have

$$247246104 = 38 \cdot 6402768 + 3940920$$
$$6402768 = 1 \cdot 3940920 + 2461848$$
$$3940920 = 1 \cdot 2461848 + 1479072$$
$$2461848 = 1 \cdot 1479072 + 982776$$
$$1479072 = 1 \cdot 982776 + 496296$$
$$982776 = 1 \cdot 496296 + 486480$$
$$496296 = 1 \cdot 486480 + 9816$$
$$486480 = 49 \cdot 9816 + 5496$$
$$9816 = 1 \cdot 5496 + 4320$$
$$5496 = 1 \cdot 4320 + 1176$$
$$4320 = 3 \cdot 1176 + 792$$
$$1176 = 1 \cdot 792 + 384$$
$$792 = 2 \cdot 384 + 24$$
$$384 = 16 \cdot \underbrace{24} \quad \textbf{(remainder =0)}$$

$$(A, B) = 24$$

Working backward,

$$\begin{aligned}
24 &= 792 - 2 \cdot 384 \\
&= -2 \cdot 1176 + 3 \cdot 792 \\
&= 3 \cdot 4320 - 11 \cdot 1176 \\
&= -11 \cdot 5496 + 14 \cdot 4320 \\
&= 14 \cdot 9816 - 25 \cdot 5496 \\
&= -25 \cdot 486480 + 1239 \cdot 9816 \\
&= 1239 \cdot 496296 - 1264 \cdot 486480 \\
&= -1264 \cdot 982776 + 2503 \cdot 496296 \\
&= 2503 \cdot 1479072 - 3767 \cdot 982776 \\
&= -3767 \cdot 2461848 + 6270 \cdot 1479072 \\
&= 6270 \cdot 3940920 - 10037 \cdot 2461848 \\
&= -10037 \cdot 6402768 + 16307 \cdot 3940920 \\
&= 16307 \cdot 247246104 - 629703 \cdot 6402768
\end{aligned}$$

Multiplicative Inverse Modulo N

To find a solution of the equation

$$A \cdot X = 1 \qquad (\text{mod } N),$$

when the greatest common diviser $D = (A, N)$ **of** A **and** N **is equal to** 1**, find** S **and** T **such that**

$$S \cdot A + T \cdot N = 1$$

using Euclid's algorithm, and then

$$X \equiv S \qquad (\text{mod } N)$$

If $A = 1232131$ **and** $N = 32342342322$ **then**

$$\begin{aligned}
1 &= 119 - 118 \\
&= -356 + 3 \cdot 119 \\
&= 3 \cdot 475 - 4 \cdot 356 \\
&= -4 \cdot 831 + 7 \cdot 475 \\
&= 7 \cdot 1306 - 11 \cdot 831 \\
&= -11 \cdot 4749 + 40 \cdot 1306 \\
&= 40 \cdot 6055 - 51 \cdot 4749 \\
&= -51 \cdot 10804 + 91 \cdot 6055 \\
&= 91 \cdot 135703 - 1143 \cdot 10804 \\
&= -1143 \cdot 1232131 + 10378 \cdot 135703 \\
&= 10378 \cdot 32342342322 - 272413265 \cdot 1232131
\end{aligned}$$

Thus $32069929057 = 32342342322 - 272413265$ **is the inverse of** 1232131**.**

Powers Modulo N

To compute

$$C = (A^k \bmod N)$$

we use the following receipe

1) If $k = 0$ then

$$C = 1$$

2) If k is odd then first compute

$$B = (A^{k-1} \bmod N)$$

and then

$$C = (A \cdot B \bmod N)$$

3) If k is even then first compute

$$B = (A^{k/2} \bmod N)$$

and then

$$C = (B^2 \bmod N)$$

For example, with $N = 32423333$,

$$(2^{12321} \bmod N) = (2 \cdot (2^{12320} \bmod N) \bmod N)$$

$$(2^{12320} \bmod N) = ((2^{6160} \bmod N)^2 \bmod N)$$

$$(2^{6160} \bmod N) = ((2^{3080} \bmod N)^2 \bmod N)$$

$$(2^{3080} \bmod N) = ((2^{1540} \bmod N)^2 \bmod N)$$

$$(2^{1540} \bmod N) = ((2^{770} \bmod N)^2 \bmod N)$$

$$(2^{770} \bmod N) = ((2^{385} \bmod N)^2 \bmod N)$$

$$(2^{385} \bmod N) = (2 \cdot (2^{384} \bmod N) \bmod N)$$

$$(2^{384} \bmod N) = ((2^{192} \bmod N)^2 \bmod N)$$

$$(2^{192} \bmod N) = ((2^{96} \bmod N)^2 \bmod N)$$

$$(2^{96} \bmod N) = ((2^{48} \bmod N)^2 \bmod N)$$

$$(2^{48} \bmod N) = ((2^{24} \bmod N)^2 \bmod N)$$

$$(2^{24} \bmod N) = ((2^{12} \bmod N)^2 \bmod N)$$

$$(2^{12} \bmod N) = ((2^{6} \bmod N)^2 \bmod N)$$

$$(2^{6} \bmod N) = ((2^{3} \bmod N)^2 \bmod N)$$

$$(2^{3} \bmod N) = (2 \cdot (2^{2} \bmod N) \bmod N)$$