Two integers m, n are coprime if $\gcd(m,n) = 1$.

e.g. 3, 7 are coprime

4, 9 are coprime

6, 21 are not coprime

Defn We let $\phi(n)$ denote the number of integers in the range $1, 2, \ldots, n$ that are coprime to n.

Example $\phi(8) = 4$

① 2 ③ 4 ⑤ 6 ⑦ 8

$\phi(6) = 2$

① 2 3 4 ⑤ 6

$\phi(107) = 106$

$\phi(19) = 18$

We call $\phi(n)$ Euler's phi function or Euler's Totient function.

Proposition 1 If p is a prime integer then $\phi(p) = p-1$.

$\phi(2^2) = 2 = 2^2 - 2^1$

$\phi(3^2) = 6 = 3^2 - 3^1$

① ② 3 ④ ⑤ 6 ⑦ ⑧ 9

$\phi(2^4) = 8 = 2^4 - 2^3$

① 2 ③ 4 ⑤ 6 ⑦ 8 ⑨ 10 ⑪ 12 ⑬ 14 ⑮ 16

Proposition 2 If p is prime then

$$\phi(p^n) = p^n - p^{n-1}$$

$\phi(3.5) = \phi(15) = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

$\phi(3) = 2$

$\phi(5) = 4$

Proposition 3 If $\gcd(m,n) = 1$ then

$$\phi(m.n) = \phi(m)\,\phi(n).$$

$\phi(4.6) = 8$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

$\phi(4) = 2$

$\phi(6) = 2$

$\phi(4.6) \neq \phi(4)\,\phi(6)$

220
110
55
11

Example

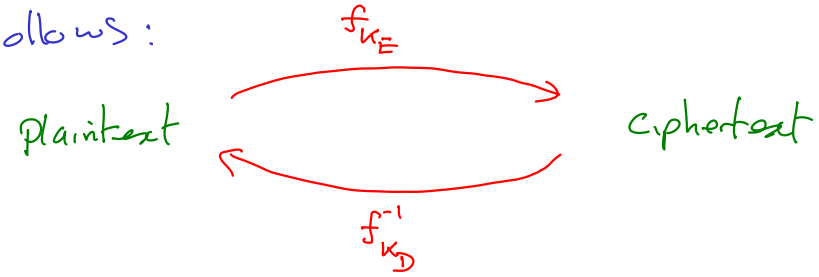
$$\phi(220) = \phi(2^2.5.11)$$
$$= \phi(2^2)\,\phi(5)\,\phi(11)$$
$$= (2^2-2^1)(5-1)(11-1)$$
$$= 2.4.10$$
$$= 80$$

Public Key Cryptography

Defn (Diffie & Hellman 1976, James Ellis a few years earlier)
A public key cryptosystem is a cryptosystem with the property that someone who knows only the enciphering key can not (without a prohibitively length calculation) discover how to decipher.

Affine cryptosystems are not public key.

Example We could use a public key cryptosystem as follows:



K_E = enciphering key (public)
K_D = deciphering key (secret)

I want to email my bank for €1000. The bank must verify that I really am Graham Ellis. To do this, the bank chooses a secret word.

Bananas

The bank looks at my webpage and looks up my public enciphering key. The bank emails me the text

$$f_{K_E}(\text{Bananas})$$

I have to tell the bank by email that the secret word is

$$f^{-1}_{K_D}\left(f_{K_E}(\text{Bananas})\right) = \text{Bananas}.$$

Only Graham Ellis can do this, as only he knows the deciphering key.

Llanfairpwllgwyngyllgogerychwyrndrobwllllantysiliogogogoch