Composite Integers Page 171

$a^{n-1} \not\equiv 1 \pmod{n} \Rightarrow n$ is composite.

Example Lilo page 172 $= n$ $n \nmid a$

Test whether 511 is composite

Soln: Using the above we have with $a=2$.

$$2^{511-1} \equiv 2^{510} \equiv x \pmod{511}$$

Computing some simple powers of 2:

$2^7 \equiv 128$, $2^8 \equiv 256$, $2^9 \equiv 512 \equiv 1 \pmod{511}$

By the D.A.

$$510 = (56 \times 9) + 6$$

Therefore

$$2^{510} \equiv 2^{(56\times 9)+6}$$
$$\equiv (2^9)^{56} 2^6$$
$$\equiv 1^{56} \times 2^6$$
$$\equiv 2^6 \equiv 64 \not\equiv 1 \pmod{511}$$

$\Rightarrow$ 511 is composite.

Example 4.13 Page 174

Show that 91 is a base 3 pseudoprime.

Soln: (I) 91 is composite

(II) $3^{90} \equiv 1 \pmod{91}$

(I) $91 = 7 \times 13$

(II) Compute some simpler powers of 3:

$$3^4 \equiv 81 \equiv -10,$$

$$3^5 \equiv 3^4 \times 3 \equiv -10 \times 3 \equiv -30 \pmod{91}$$

$$3^6 \equiv 3^5 \times 3^1 \equiv -30 \times 3$$

$$\equiv -90 \equiv 1 \pmod{91}$$

Using this result $3^6 \equiv 1 \pmod{91}$

$$3^{90} \equiv 3^{6 \times 15}$$

$$\equiv (3^6)^{15} \equiv 1 \pmod{91}$$

Proposition (4.9) If $m|n$ then $(2^m-1)|(2^n-1)$.

Proof: we are given $m|n \Rightarrow m \times k = n$.

$$a^{r\times s}-1 = (a^r-1)\left[a^{r(s-1)} + a^{r(s-2)} + \cdots + a^r + 1\right]$$

$$2^n-1 = 2^{m\times k}-1 = (2^m-1)\left[2^{m(k-1)} + 2^{m(k-2)} + \cdots + 2^m + 1\right]$$

$$\Rightarrow (2^m-1)|(2^n-1).$$

Ex 4.14 $2^{18}-1 = 262\,143$.

Factors of 18 are 2, 3, 6, 9.

$2^2-1=3 \Rightarrow 3|(2^{18}-1)$

$2^3-1=7 \Rightarrow 7|(2^{18}-1)$

$2^6-1=63 \Rightarrow 63|(2^{18}-1)$

$2^9-1=511 \Rightarrow 511|(2^{18}-1)$

Therefore $\frac{2^{18}-1}{511} = 513$ or $2^{18}-1 = 511 \times 513$ (*1)

$\frac{513}{9} = 57 = 3\times 19 \Rightarrow 513 = 3\times 9\times 19 = 3^3\times 19$

$511 = 7\times 73$

$511 = (7 \times 73)$

$2^{18} - 1 = 511 \times 513$

$= 7 \times 73 \times 3^3 \times 19$

$= 3^3 \times 7 \times 19 \times 73 = 262\,143.$