chapter 21

$b \equiv c \pmod a$ if $b-c$ div. by a

$a^m \equiv 1 \pmod p$

$p=7$ $1 < a < 7$ find m s.t. $a^m \equiv 1 \pmod 7$

$2^m \equiv 1 \pmod 7$ $p-1=6$ 1,2,3,6

$2^3 = 8 \equiv 1 \pmod 7$

$3^m \equiv 1 \pmod 7$

$3^6 = 729 \equiv 1 \pmod 7$ $7 \cdot 104 = 728$

$4^m \equiv 1 \pmod 7$

$4^3 = 64 \equiv 1 \pmod 7$

$5^m \equiv 1 \pmod 7$

$5^6 = 15625 \equiv 1 \pmod 7$ $(7 \cdot 2232 + 1)$

$6^m \equiv 1 \pmod 7$

$6^2 \equiv 1 \pmod 7$

$a^{p-1} \equiv 1 \pmod p$

$a^{(p-1)/2} \equiv -1 \pmod p$ $(p-1)/2$ must be smallest exponent!

$1^6 \equiv 1 \pmod{13}$ $(-1)^6 = 1 \equiv 1 \pmod{13}$

$2^6 = 64 \equiv -1 \pmod{13}$ (& 11!)

$3^6 = 729 \equiv 1 \pmod{13}$

$56 \times 13 = 728$

$81 \times 3 = 243 \times 3 = 729$

$(-2)^6 = 64 \equiv -1 \pmod{13}$

$-2 \equiv 11 \pmod{13}$

$(11)^6 = 1771561 = (136274 \times 13) - 1$

$4^6 = 4096 \equiv 1 \pmod{13}$

$4 \times 4 = 16 \times 4 = 64 \times 4 = 256 \times 4 = 1024 \times 4 = 4096$

$(315 \times 13 = 4095)$

4 not P.R. $\Rightarrow -4$ not P.R.

$-4 \equiv 9 \pmod{13} \Rightarrow 9$ not P.R.

3 not P.R $\Rightarrow 10$ not P.R.

1 not P.R. $\Rightarrow 12$ not P.R.

$5^6 = 15625 \equiv -1 \pmod{13}$ $(1202 \cdot 13 - 1)$

but wait, there's more!

$5^2 = 25 = 26 - 1 \equiv -1 \pmod{13}$

5 not P.R. $\Rightarrow 8$ not P.R.

$6^6 = 46656 \equiv -1 \mod 13$ ←

$6^2 = 36 \equiv 10 \mod 13$

$6^3 = 216 \equiv 8 \mod 13$

6 is P.R. $-6 \equiv 7 \pmod{13}$

7 also P.R.

2, 6, 7, 11

$$x^n - 1 = 0$$

$$(x-1)(x^{n-1} + x^{n-2} + \dots + x + 1) = 0$$

Galois: 3 real roots & 2 complex roots

$$x^5 - 3x + 2$$