Lecture 26
March 13th, 2015

Chapter 29
Chapter 31–32
35-36 Primitive roots & indices g = primitive root mod p
$\{g, g^2, \cdots, g^{p-1} \bmod p\}$
$= \{1, 2, \cdots, p-1 \bmod p\}$
i.e. for $1 \le a < p$, $a \equiv g^k \bmod p$ for some k
Define $k = I(a)$: index of a mod p for the base g.

$p=13$. 2 is a primitive root.

I	1	2	3	4	5	6	7	8	9	10	$\boxed{11}$	12
2^I	2	4	8	3	6	12	11	9	5	10	$\boxed{7}$	1

$2^5 = 32 \equiv 6 \bmod 13$

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

$I(7) = 11$, $7 = 2^{11} \bmod 13$

Index Rules theorem: (a) Product Rule : $I(ab) = I(a) + I(b) \bmod p-1$
(b). Power Rule : $I(a^k) = kI(a) \bmod p-1$
$I(a)$ behaves like logarithm
$\downarrow$
called discrete logarithm

Proof: $g^{I(ab)} \equiv ab \equiv g^{I(a)} g^{I(b)} \equiv g^{I(a)+I(b)} \bmod p$
$I(ab) \equiv I(a) + I(b) \bmod p-1$
$g^{I(a^k)} \equiv a^k \equiv (g^{I(a)})^k = g^{kI(a)} \bmod p$
$I(a^k) \equiv kI(a) \bmod p-1$

$g=2$, $p=37$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$I(a)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17

a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$I(a)$	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

e.g. $29^{14} \bmod 37$
successive squaring may be easier
$I(29^{14}) \equiv 14\, I(29) \bmod 36$
$\equiv 14 \times 21 \equiv 6 \bmod 36$
So $29^{14} \equiv 27 \bmod 37$

$19x \equiv 23 \bmod 37$? Method ① Ch 8. $\gcd(19, 37) = 1$, $19 \times 2 - 37 = 1$, $x = 2 \times 23 = 46 \equiv 9 \bmod 37$
Method ②: $I(19) + I(x) \equiv I(19x) \equiv I(23) \bmod 36$
$35 + I(x) \equiv 15 \bmod 36$
$I(x) \equiv -20 \equiv 16 \bmod 36 \Rightarrow x \equiv 9 \bmod 37$

But for these (only index works):

$3\cdot x^{30} \equiv 4 \mod 37$

$I(3\cdot x^{30}) \equiv I(4) \mod 36$

$\parallel\!|$

$I(3) + 30I(x)$

$26 + 30I(x) \equiv 2 \mod 36$

$30I(x) \equiv -24 \equiv 12 \mod 36$

$\gcd(30, 36) = 6,\ 6|12$

there are 6 incongruent solutions.

To solve $30y \equiv 12 \mod 36$

$30x - 36k = 6$

$x = -1$

$y = -2 + 6n$, where $n = \cancel{0}, 1, 2, 3, 4, 5, 6$

so $I(x) \equiv 4, 10, 16, 22, 28, 34 \mod 36$

then $x \equiv 16, 25, 9, 21, 12, 28 \mod 37$

Last time proof:

If $m = p_1 \cdots p_r$, $p_i \equiv 1 \mod 4 \rightsquigarrow m = a^2 + b^2$, $\gcd(a,b) = 1$

$= p_1^{k_1} \cdots p_r^{k_r}$, p_i distinct prime

m is a prime power $\Rightarrow$ can be written as sum of two $\square$'s.

$$\left.\begin{array}{l} m = r\cdot s,\ \gcd(r,s) = 1 \\ \quad r = a^2 + b^2,\ \gcd(a,b) = 1 \\ \quad s = c^2 + d^2,\ \gcd(c,d) = 1 \end{array}\right\} \Rightarrow m = A^2 + B^2,\ \gcd(A, B) = 1$$

$m = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$

claim: $\gcd(ac - bd, ad + bc) = 1$

Suppose $q | ac - bd$, $q | ad + bc$, q prime

$q \nmid a$, $q \nmid$, $q \nmid c$, $q \nmid d$, [Why not? If $q | a$, $q | d$, $q | c$ contradiction]

so $ad + bc \equiv 0 \mod q$

$ad \equiv -bc \mod q$ & $ac \equiv bd \mod q$

$adc \equiv -bc^2 \mod q$

$\equiv bd^2 \mod q$

so $b(c^2 + d^2) \equiv 0 \mod q \longrightarrow q | c^2 + d^2$

Similarly (by multipling a both sides, $q | a^2 + b^2$

Therefore we have a $\Rightarrow\!\Leftarrow$