Handout (Sections 7.4 & 7.3)

① Illustration of the proof of "$n = \sum_{d|n} \phi(d)$"

$n=10$, divisors of 10 are 1, 2, 5, 10

so,
$S_1 = \{1, 3, 7, 9\}$ (note: $\phi(\frac{10}{1})=4$)
$S_2 = \{2, 4, 6, 8\}$ ($\phi(\frac{10}{2}) = \phi(5) = 4$)
$S_5 = \{5\}$ ($\phi(\frac{10}{5}) = \phi(2) = 1$)
$S_{10} = \{10\}$ ($\phi(1)=1$) together partition $\{1, 2, 3, \ldots, 10\}$ into four parts.

Therefore, $\sum_{d|10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1)$
$= 4+4+1+1 = 10.$

② Another proof of "$n = \sum_{d|n} \phi(d)$"

Proof Let $F(n) = \sum_{d|n} \phi(d)$. Since ϕ is mult., by Thm. F is also mult.

Consider $F(p^k)$, p^k prime power

$F(p^k) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^k)$
$= 1 + (p-1) + (p^2-p) + \cdots + (p^k - p^{k-1})$
$= p^k$

Let $n = p_1^{k_1} \cdots p_r^{k_r}$ (assuming $n>1$; for $n=1$: $1 = \phi(1)$)

$F(n) = F(p_1^{k_1} \cdots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r})$
$= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = n.$

③ We can use Euler's Thm. to find 11^{29} modulo 30 even though 30 is not prime.

By Euler, $11^8 \equiv 1 \pmod{30}$ ($\because \phi(30)=8$ & $\gcd(11,30)=1$)

$11^{29} = (11^8)^3 \cdot 11^5 \equiv (1)^3 \cdot 11^5 \equiv 11 \pmod{30}$

④ Find units digit of 3^{100}

Since $\gcd(3,10)=1$, & $\phi(10)=4$, $3^4 \equiv 1 \pmod{10}$

$\therefore 3^{100} = (3^4)^{25} \equiv (1)^{25} \equiv 1 \pmod{10}$. Hence units digit is 1.

⑤ For any integer a, $a^{37} \equiv a \pmod{1729}$?

Note $1729 = 7 \cdot 13 \cdot 19$ (remember this number?)

If $\gcd(a,19)=1$, then $a^{\phi(19)} \equiv 1 \pmod{19}$, i.e. $a^{18} \equiv 1 \pmod{19}$

or $a^{36} \equiv 1 \pmod{19}$ by squaring

or $a^{37} \equiv a \pmod{19}$

If $19 | a$, then $a^{37} \equiv a \pmod{19}$

So, $a^{37} \equiv a \pmod{19}$ for all a. —①

If $\gcd(a,13)=1$, then $a^{\phi(13)} = a^{12} \equiv 1 \pmod{13}$

or $a^{36} \equiv 1 \pmod{13}$ by cubing

or $a^{37} \equiv a \pmod{13}$

If $13 | a$, then $a^{37} \equiv a \pmod{13}$

So, $a^{37} \equiv a \pmod{13}$ for all a. —②

If $\gcd(a,7)=1$, then $a^{\phi(7)} = a^{6} \equiv 1 \pmod{7}$

or $a^{36} \equiv 1 \pmod{7}$ by taking 6^{th} powers

or $a^{37} \equiv a \pmod{7}$

If $7 | a$ then $a^{37} \equiv a \pmod{7}$

So, $a^{37} \equiv a \pmod{7}$ for all a —③

Since, 7, 13 & 19 are pairwise co-prime,

we get $a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}$.

⑥ Find the last two digits of 3^{256}

Since $\gcd(3,100)=1$, & $\phi(100) = \phi(2^2 \cdot 5^2) = 40$,

$3^{40} \equiv 1 \pmod{100}$ —①

Since $256 = 6 \cdot 40 + 16$, $3^{256} = 3^{6 \cdot 40 + 16} = (3^{40})^6 \, 3^{16}$

$\equiv 3^{16} \pmod{100}$

$3^2 \equiv 9 \pmod{100} \Rightarrow 3^4 \equiv 81 \pmod{100}$

$\Downarrow$

$3^{16} \equiv 21 \pmod{100} \Leftarrow 3^8 \equiv 61 \pmod{100}$

$\therefore$ 21 are the last two digits.