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, 3, 5, 10

So, $S_1 = \{1\}$ (note: $\phi(1) = 1$)

$S_2 = \{2\}$ (note: $\phi(2) = 1$)

$S_5 = \{5\}$ (note: $\phi(5) = 1$)

$S_{10} = \{10\}$ (note: $\phi(10) = 4$)

Together partition $\{1, 2, 3, ..., 10\}$ into 4 parts.

Therefore, $\sum_{d|n} \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 $\phi$ is multiplicative, by Thm. $F$ is also multiplicative.

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

$F(p^k) = \sum_{d|p^k} \phi(d) = \phi(p) + \phi(p^2) + \ldots + \phi(p^k)

= 1 + (p-1) + (p^2 - p) + \ldots + (p^k - p^{k-1})

= p^k - 1$

Let $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m}$ (assuming $n > 1$; for $n = 1$: $1 = \phi(1)$)

$F(n) = F(p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}) = F(p_1^{k_1}) \cdot F(p_2^{k_2}) \cdot \ldots \cdot F(p_m^{k_m})

= p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} = n$

3. We can use $\phi$ to find $11^{29}$ modulo 30 even though 30 is not prime.

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

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

4. Find units digit of $3^{100}$

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

$3^{100} = (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{10}$.

Hence, the units digit is 1.
5. For any integers $a$, $a^{37} \equiv a \pmod{1729}$?  

Note 1729 = 7.13.19 (remember this number?)

By Fermat's Little Theorem, if $\gcd(a, 19) = 1$, then $a^{18} \equiv 1 \pmod{19}$, i.e., $a^{18} = 1 \pmod{19}$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Since 7, 13, and 19 are pairwise coprime, we get $a^{37} \equiv a \pmod{7.13.19}$

6. Find the last two digits of $3^{256}$

Since $\gcd(3, 100) = 1$, \& $\phi(100) = \phi(2^2.5^2) = 40$,

$3^{40} \equiv 1 \pmod{100}$ \(\text{(1)}\)

Since $256 = 6.40 + 16$, $3^{256} = 3^{6.40+16} = (3^{40})^6.3^{16}$

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

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

$3^8 \equiv 61 \pmod{100}$

$3^{16} \equiv 61 \pmod{100}$

The last two digits are 81.