Euler $\varphi$ (totient) function and arithmetic mod $m$

An integer is an element of the set \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}; $(a, b)$ is the greatest common divisor of integers $a, b$. For example, $(10, 8) = (6, 16) = 2$, $(5, 6) = (4, 9) = 1$. Two integers $a, b$ are called relatively prime if and only if $(a, b) = 1$. Notation $d|a$ means $d$ divides $a$. In particular, for every non-zero integers $a, a|0$, $a|a$, and $(a, 1) = 1$.

**Definition.** The Euler $\varphi$, or totient, function is defined, for integer $n \geq 1$, by

$$\varphi(n) = \text{the number of integers in the range } [1, n] \text{ that are relatively prime to } n.$$  

**Examples.**

1. $\varphi(5) = 4$ (the numbers $1, 2, 3, 4$ are relatively prime to $5$, but $5$ is not).
2. $\varphi(10) = 4$ (the numbers $1, 3, 7, 9$ are relatively prime to $10$, but $2, 4, 5, 6, 8, 10$ are not.)

**Fact:** If $n = p_1^{k_1} \cdots p_m^{k_m}$, where $p_1, \ldots, p_m$ are distinct prime divisors of $n$ and $k_i \geq 1$, then

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

In particular, if $n = p$ is prime, then $\varphi(n) = p - 1$ and if $n = n_1n_2$, where $(n_1, n_2) = 1$, that is, $n_1$ and $n_2$ are relatively prime, then $\varphi(n) = \varphi(n_1)\varphi(n_2)$. **Example.** $\varphi(72) = \varphi(2^3 \cdot 3^2) = 72(1 - 1/2)(1 - 1/3) = 72/3 = 24$.

**Definition.** For integer numbers $a, b, m$, notation $a \equiv b \pmod{m}$ means $a - b$ is divisible by $m$, that is $m|(a - b)$ or, equivalently, $a - b = km$ for some integer $k$.

Direct computations show that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$ and $a_1a_2 \equiv b_1b_2 \pmod{m}$. In particular, if $a \equiv b \pmod{m}$, then $ka \equiv kb \pmod{m}$ for every integer $k$ and $a^n \equiv b^n \pmod{m}$ for every positive integer $n$. As a result, if $a \equiv b \pmod{m}$ and $P = P(x)$ is a polynomial with integer coefficients, then $P(a) \equiv P(b) \pmod{m}$.

**Example.** If $P(x) = 3x^7 - 41x^2 - 91x$, then $P(x) \equiv 3x^7 - 2x^2 \pmod{13}$ and $P(11) \equiv 11 \pmod{13}$ (because $11 \equiv -2 \pmod{13}$).

If $(k, m) = 1$, then $ka \equiv kb \pmod{m}$ implies $a \equiv b \pmod{m}$. If $d|a$, $d|b$, and $d|m$, then $a \equiv b \pmod{m}$ implies $(\frac{a}{d}) \equiv (\frac{b}{d}) \pmod{\frac{m}{d}}$.

**Example.** $30 \equiv 60 \pmod{6}$, which implies $6 \equiv 12 \pmod{6}$, $15 \equiv 30 \pmod{3}$, and $10 \equiv 20 \pmod{2}$.

If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$. More generally, if $(m_i, m_j) = 1$, $i, j = 1, \ldots, k$, then

$$a \equiv b \pmod{m_i}, \quad i = 1, \ldots, k$$

if and only if

$$a \equiv b \pmod{m_1 \cdots m_k}.$$
Even more generally, for arbitrary integer $m_1, \ldots, m_k$,
\[ a \equiv b \pmod{m_i}, \quad i = 1, \ldots, k \text{ if and only if } a \equiv b \pmod{[m_1 \cdots m_k]}, \]
where $[m_1 \cdots m_k]$ is the least common multiple of $m_1, \ldots m_k$.

**Example.** $38 \equiv 110 \pmod{4}$, $38 \equiv 110 \pmod{9}$, and $38 \equiv 110 \pmod{12}$ is equivalent to $38 \equiv 110 \pmod{36}$.

**Theorem.** If $(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Indeed, let $x_1, \ldots, x_{\varphi(m)}$ be the integers from the interval $[1, m]$ that are relatively prime to $m$. Then, for each $i = 1, \ldots, \varphi(n)$, $ax_i$ is also relatively prime to $m$ and so there exists $j$ so that $ax_i \equiv x_j \pmod{m}$. Consequently, $a^{\varphi(m)}x_1 \cdots x_{\varphi(m)} \equiv x_1 \cdots x_{\varphi(m)} \pmod{m}$, and the result follows.

**Corollary 1.** If $p$ is a prime number, then $a^p \equiv a \pmod{p}$ for every integer $a$.

**Note.** If $(a, m) > 1$, then, in general, $a^{\varphi(m)+1} \not\equiv a \pmod{m}$. For example, with $a = 2$ and $m = 4$, we find $\varphi(4) = 2$, but $2^3 \not\equiv 2 \pmod{4}$.

**Corollary 2.** If $(a, m) = 1$ and $ax \equiv b \pmod{m}$, then $x \equiv ba^{\varphi(m)-1} \pmod{m}$.

**Examples.**

1. (92A3) For fixed integer $m$, find integer $(x, y, n)$ so that $(m, n) = 1$ and $(x^2 + y^2)^n = (xy)^n$.
2. (88B1) Show that every positive composite (that is, not prime) number can be written as $xy + yz + zx + 1$ for some positive integers $x, y, z$.
3. (86A2) What is the right-most digit of the number
\[ \left\lfloor \frac{10^{20000}}{10^{100} + 3} \right\rfloor ? \]
([a] means the largest integer less than or equal to a.)
4. (69B1) For a positive integer $n$ show that if $24|n+1$, then $24|\sum_{d|n} d$. 

**Problems.**

1. (92A3) For fixed integer $m$, find integer $(x, y, n)$ so that $(m, n) = 1$ and $(x^2 + y^2)^n = (xy)^n$.
2. (91B4) For an odd prime $p$, show that
\[ \sum_{j=0}^{p} \binom{p}{j} \left( \frac{p+j}{j} \right) \equiv 2p + 1 \pmod{p^2}. \]
3. (88B1) Show that every positive composite (that is, not prime) number can be written as $xy + yz + zx + 1$ for some positive integers $x, y, z$.
4. (86A2) What is the right-most digit of the number
\[ \left\lfloor \frac{10^{20000}}{10^{100} + 3} \right\rfloor ? \]
([a] means the largest integer less than or equal to a.)
5. (69B1) For a positive integer $n$ show that if $24|n+1$, then $24|\sum_{d|n} d$. 