Theorem 103.

(a) $\phi(n) = n - 1$ if and only if n is a prime.

(b) If p is a prime, then $\phi(p^k) = p^k - \frac{p^k}{p} = p^k\left(1 - \frac{1}{p}\right)$.

(c) ϕ is multiplicative, that is, $\phi(nm) = \phi(n)\phi(m)$ whenever n, m are coprime.

(d) Hence, if the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

Proof.

(a) $\phi(n) = n - 1$ if and only if n doesn't share a common factor with any of $\{1, 2, \ldots, n-1\}$. That's true for n precisely when it is a prime.

(b) If p is a prime, then $n = p^k$ is coprime to all $\{1, 2, \ldots, p^k\}$ except $p, 2p, \ldots, p^k$.

(c) Note that a is invertible modulo nm if and only if a is invertible modulo both n and m.
The claim therefore follows from the Chinese remainder theorem which provides a bijective (i.e., 1-1 and onto) correspondence

$$x \pmod{nm} \mapsto \begin{bmatrix} x \pmod{n} \\ x \pmod{m} \end{bmatrix}.$$

Alternatively, our book contains a direct proof (page 133).

(d) Using the two previous parts, we have
$\phi(n) = \phi(p_1^{k_1}) \cdots \phi(p_r^{k_r}) = p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$. □

For instance. Let's make the correspondence provided by the Chinese remainder theorem explicit for $n = 2$, $m = 3$: $0 \to \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $1 \to \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, $2 \to \begin{bmatrix} 0 \\ 2 \end{bmatrix}$, $3 \to \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $4 \to \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $5 \to \begin{bmatrix} 1 \\ 2 \end{bmatrix}$

Example 104. Compute $\phi(1000)$.

Solution. $\phi(1000) = \phi(2^3 \cdot 5^3) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$.

Example 105. Compute $\phi(980)$.

Solution. $\phi(980) = \phi(2^2 \cdot 5 \cdot 7^2) = 980\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 336$.

Theorem 106. (Euler's theorem) If $n \geqslant 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Before, we prove Euler's theorem, let us review Fermat's little theorem, which is the special case of prime n.

Fermat's little theorem. If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. (Fermat's little theorem) The first $p - 1$ multiples of a,

$$a, 2a, 3a, \ldots, (p-1)a$$

are all different modulo p. Clearly, none of them is divisible by p.
Consequently, these values must be congruent (in some order) to the values $1, 2, \ldots, p-1$ modulo p. Thus,

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p}.$$

Cancelling the common factors (allowed because p is prime!), we get $a^{p-1} \equiv 1 \pmod{p}$. □

Armin Straub
straub@southalabama.edu

Proof. (Euler's theorem) Let $m_1, m_2, \ldots, m_d$ be the values among $\{1, 2, \ldots, n-1\}$ which are coprime to n. Then,

$$am_1, am_2, am_3, \ldots, am_d$$

are all different modulo n. Clearly, none of them share a common factor with n.
Consequently, these values must be congruent (in some order) to the values $m_1, m_2, \ldots, m_d$ modulo n. Thus,

$$am_1 \cdot am_2 \cdot am_3 \cdot \ldots \cdot am_d \equiv m_1 \cdot m_2 \cdot m_3 \cdot \ldots \cdot m_d \pmod{n}.$$

Cancelling the common factors (allowed because the m_i are invertible $\bmod n$), we get $a^d \equiv 1 \pmod{n}$. □

Example 107. Compute $7^{100} \pmod{60}$.

Solution. $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16$. Since $\gcd(7, 60) = 1$, we obtain that $7^{16} \equiv 1 \pmod{60}$ by Euler's theorem. Since $100 \equiv 4 \pmod{16}$, we have $7^{100} \equiv 7^4 \pmod{60}$.

[because $100 = 4 + 16m$ for some m, and so $7^{100} = (7^{16})^m \cdot 7^4 \equiv 7^4 \pmod{60}$]

It remains to notice that $7^2 = 49 \equiv -11$ and hence $7^4 \equiv (-11)^2 = 121 \equiv 1 \pmod{60}$. So, $7^{100} \equiv 1 \pmod{60}$.

Example 108. (another joke) Why do mathematicians confuse Halloween and Christmas?

Because 31 Oct = 25 Dec.

Get it? $(31)_8 = 1 + 3 \cdot 8 = 25$ equals $(25)_{10} = 25$.

5.4 Primality testing

Recall that it is extremely difficult to factor large integers (this is the starting point for cryptography). Surprisingly, it is much simpler to tell if a number is a prime or composite (without factoring it). The following is a first hint at how this can be done.

By Fermat's little theorem, if p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a. On the other hand, this congruence is usually false if p is not a prime.

Example 109. Is 35 a prime? (Of course, not.)

Solution. If 35 was a prime, then $2^{35} \equiv 2 \pmod{35}$. Let's check!

$2^1 = 2$, $2^2 = 4$, $2^4 = 16$, $2^8 = 16^2 \equiv 11$, $2^{16} \equiv 11^2 \equiv 16$, $2^{32} \equiv 16^2 \equiv 11$.

Hence, $2^{35} \equiv 2^{32} \cdot 2^2 \cdot 2^1 \equiv 11 \cdot 4 \cdot 2 \equiv 18 \not\equiv 2 \pmod{35}$. This implies that 35 is not a prime!

Note. We showed that 35 is not a prime without factoring it! Our method here certainly seems more complicated than trying to find these factors, but the situation is the opposite when the numbers get large.

Also note. If 2^{35} had worked out to be congruent to 2 modulo 35, then we wouldn't have learned anything: 35 might be a prime, or it might not. Repeating such tests, however, we can build more and more confidence that our number is a prime. This uncertainty is a common feature of the most efficients primality tests, which are heuristic: they either prove that our number is not a prime or conclude that it "very likely" is a prime.

Comment. Our computation simplifies a little bit using Euler's theorem: $\phi(35) = 35\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right) = 24$. Hence, $2^{35} \equiv 2^{11} \equiv 11 \cdot 4 \cdot 2 \equiv 18 \pmod{35}$. However, in order to use this, we needed to know the prime factorization of 35, which defeats the present purpose (since that means we already know that p is not a prime).

Example 110. (homework)

- Evaluate $\phi(2016)$.
- Evaluate $\phi(10^n)$.
- Use Euler's theorem to compute $2^{666} \pmod{77}$.
- For any integer a, show that a and a^{4n+1} have the same last (decimal) digit.
- Use Euler's theorem to show that $51 | (10^{32n+9} - 7)$ for any integer $n \geqslant 0$.