Example 113. Recall that **Fermat's last theorem** states that $x^n + y^n = z^n$ does not have any solutions in positive integers if $n \geqslant 3$.

However, in a Simpson's episode, Homer discovered that

$$1782^{12} + 1841^{12} \text{ “}{=}\text{” } 1922^{12}.$$

If you check this on an old calculator it might confirm the equation. However, the equation is not correct, though it is “nearly”: $1782^{12} + 1841^{12} - 1922^{12} \approx -7.002 \cdot 10^{29}$.

Why would that count as “nearly”? Well, the smallest of the three numbers, $1782^{12} \approx 1.025 \cdot 10^{39}$, is bigger by a factor of more than 10^9. So the difference is extremely small in comparison.

Relative errors. If you estimate x with y, the **absolute error** is $|x - y|$. However, for many applications, the **relative error** $\left|\frac{x-y}{x}\right|$ is much more important.

Check! Show that Homer is wrong by hand by looking at this modulo 13. (Though modulo 2 is even easier!)

Solution. By Fermat's little theorem, we have $x^{12} \equiv 1 \pmod{13}$ for all x not divisible by 13. Our numbers are not divisible by 13. Hence, $1782^{12} + 1841^{12} \equiv 2 \pmod{13}$ but $1922^{12} \equiv 1 \pmod{13}$, so they cannot be equal.

http://www.bbc.com/news/magazine-24724635

12 Euler's theorem

Theorem 114. (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 $a^{p-1} \equiv 1 \pmod{p}$. □

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. Note that $d = \phi(n)$ and that these are precisely the invertible residues modulo n. Observe that the residues

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

are all invertible (why?!) modulo n and different from each other.

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 $a^d \equiv 1 \pmod{n}$. □

Armin Straub
straub@southalabama.edu

Example 115. Compute $37^{101} \pmod{35}$.

Solution. First, note that $37^{101} \equiv 2^{101} \pmod{35}$.

$\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$. Since $\gcd(2, 35) = 1$, we obtain that $2^{24} \equiv 1 \pmod{35}$ by Euler's theorem (in other words, we can reduce modulo 24 in the exponent).

Since $101 \equiv 5 \pmod{24}$, we have $2^{101} \equiv 2^5 = 32 \equiv -3 \pmod{35}$.

Example 116. What are the last two (decimal) digits of 3^{4242}?

Solution. We need to determine $3^{4242} \pmod{100}$. $\phi(100) = \phi(2^2) \cdot \phi(5^2) = (4-2)(25-5) = 40$.

Since $\gcd(3, 100) = 1$ and $4242 \equiv 2 \pmod{40}$, Euler's theorem shows that $3^{4242} \equiv 3^2 = 9 \pmod{100}$.

Therefore the last two digits are 09.

Example 117. Compute $7^{102} \pmod{60}$.

Solution. $\phi(60) = \phi(2^2)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$. Since $\gcd(7, 60) = 1$, we obtain that $7^{16} \equiv 1 \pmod{60}$ by Euler's theorem. Since $102 \equiv 6 \pmod{16}$, we have $7^{102} \equiv 7^6 \pmod{60}$.

It then follows from $7^2 \equiv -11$, $7^4 \equiv (-11)^2 \equiv 1 \pmod{60}$ that $7^{102} \equiv 7^6 \equiv 7^4 \cdot 7^2 \equiv 1 \cdot (-11) \equiv -11 \pmod{60}$.

13 Multiplicative order and primitive roots

Example 118. (warmup) Compute the powers of 2 modulo 11.

Solution. $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 5, 2^5 \equiv 2 \cdot 5 = 10, 2^6 \equiv 2 \cdot 10 \equiv 9, 2^7 \equiv 2 \cdot 9 \equiv 7, 2^8 \equiv 2 \cdot 7 \equiv 3,$ $2^9 \equiv 2 \cdot 3 = 6, 2^{10} \equiv 2 \cdot 6 \equiv 1$, and now the numbers we get will repeat...

Note. By **Fermat's little theorem**, it was clear from the beginning that $2^{10} \equiv 1 \pmod{11}$. Our computation shows that $k = 10$ is the smallest exponent such that $2^k \equiv 1 \pmod{11}$. We therefore say that 2 has **multiplicative order** 10 modulo 11.

Also notice that the values $2^0, 2^1, \ldots, 2^9$, together with 0, form a complete set of residues modulo 11. For that reason, we say that 2 is a **primitive root** modulo 11.

Definition 119. The **multiplicative order** of an invertible residue a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Definition 120. If the multiplicative order of an residue a modulo n equals $\phi(n)$ [in other words, the order is as large as possible], then a is said to be a **primitive root** modulo n.

A primitive root is also referred to as a **multiplicative generator** (because the products of a, that is, $1, a, a^2,$ $a^3, \ldots$, produce all [$\phi(n)$ many] invertible residues).

Example 121. Determine the orders of each (invertible) residue modulo 7. In particular, determine all primitive roots modulo 7.

Solution. We will develop more tools next time. For now, let us just consider each residue individually and determine, by brute-force, what its order is.

- Since $2^2 = 4$, $2^3 \equiv 1$, the order of 2 is 3.
- Since $3^2 = 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$, the order of 3 is 6.

Proceeding likewise for the other residues, we find:

residue	1	2	3	4	5	6
order	1	3	6	3	6	2

In particular, the primitive roots are 3 and 5.

Review. $x \pmod{n}$ is a primitive root.

$\iff$ The (multiplicative) order of $x \pmod{n}$ is $\phi(n)$. (That is, the order is as large as possible.)

$\iff$ $x, x^2, \ldots, x^{\phi(n)}$ is a list of all invertible residues modulo n.

Lemma 122. If $a^r \equiv 1 \pmod{n}$ and $a^s \equiv 1 \pmod{n}$, then $a^{\gcd(r,s)} \equiv 1 \pmod{n}$.

Proof. By Bezout's identity, there are integers x, y such that $xr + ys = \gcd(r, s)$.
Hence, $a^{\gcd(r,s)} = a^{xr+ys} = a^{xr}a^{ys} = (a^r)^x(a^s)^y \equiv 1 \pmod{n}$. □

Corollary 123. The multiplicative order of a modulo n divides $\phi(n)$.

Proof. Let k be the multiplicative order, so that $a^k \equiv 1 \pmod{n}$. By Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$. The previous lemma shows that $a^{\gcd(k,\phi(n))} \equiv 1 \pmod{n}$. But since the multiplicative order is the smallest exponent, it must be the case that $\gcd(k, \phi(n)) = k$. Equivalently, k divides $\phi(n)$. □

Example 124. Compute the multiplicative order of 2 modulo $7, 11, 9, 15$. In each case, is 2 a primitive root?

Solution.

- $2 \pmod{7}$: $2^2 \equiv 4, 2^3 \equiv 1$. Hence, the order of 2 modulo 7 is 3.
  Since the order is less than $\phi(7) = 6$, 2 is not a primitive root modulo 7.
- $2 \pmod{11}$: Since $\phi(11) = 10$, the only possible orders are $2, 5, 10$. Hence, checking that $2^2 \not\equiv 1$ and $2^5 \not\equiv 1$ is enough to conclude that the order must be 10.
  Since the order is equal to $\phi(11) = 10$, 2 is a primitive root modulo 11.
- $2 \pmod{9}$: Since $\phi(9) = 6$, the only possible orders are $2, 3, 6$. Hence, checking that $2^2 \not\equiv 1$ and $2^3 \not\equiv 1$ is enough to conclude that the order must be 6. (Indeed, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, $2^6 \equiv 1$.)
  Since the order is equal to $\phi(9) = 6$, 2 is a primitive root modulo 9.
- The order of $2 \pmod{15}$ is 4 (a divisor of $\phi(15) = 8$).
  2 is not a primitive root modulo 15. In fact, there is no primitive root modulo 15.

Comment. It is an open conjecture to show that 2 is a primitive root modulo infinitely many primes. (This is a special case of Artin's conjecture which predicts much more.)

Advanced comment. There exists a primitive root modulo n if and only if n is of one of $1, 2, 4, p^k, 2p^k$ for some odd prime p.

Example 125. Is there a primitive root modulo 8?

Solution. Since $\phi(8) = 8 - 4 = 4$, the question is whether there is a residue of order 4.
The invertible residues are $\pm1, \pm3$. Obviously, 1 has order 1 and -1 has order 2. Since $(\pm3)^2 \equiv 1 \pmod{8}$, the residues ±3 have order 2 as well. There is no primitive root.

Armin Straub
straub@southalabama.edu

Lemma 126. Suppose $x \pmod{n}$ has (multiplicative) order k.

(a) $x^a \equiv 1 \pmod{n}$ if and only if $k|a$.

(b) $x^a \equiv x^b \pmod{n}$ if and only if $a \equiv b \pmod{k}$.

(c) x^a has order $\frac{k}{\gcd(k, a)}$.

Proof.

(a) "$\Longrightarrow$": By Lemma 122, $x^k \equiv 1$ and $x^a \equiv 1$ imply $x^{\gcd(k,a)} \equiv 1 \pmod{n}$. Since k is the smallest exponent, we have $k = \gcd(k, a)$ or, equivalently, $k|a$.
"$\Longleftarrow$": Obviously, if $k|a$ so that $a = kb$, then $x^a = (x^k)^b \equiv 1 \pmod{n}$.

(b) Since x is invertible, $x^a \equiv x^b \pmod{n}$ if and only if $x^{a-b} \equiv 1 \pmod{n}$ if and only if $k|(a-b)$.

(c) By the first part, $(x^a)^m \equiv 1 \pmod{n}$ if and only if $k|am$. The smallest such m is $m = \frac{k}{\gcd(k, a)}$. $\square$

Example 127. Redo Example 121, starting with the knowledge that 3 is a primitive root.

That is, determine the orders of each residue modulo 7.

Solution.

residues	1	2	3	4	5	6
3^a	3^0	3^2	3^1	3^4	3^5	3^3
order$=\frac{6}{\gcd(a,6)}$	$\frac{6}{6}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{2}$	$\frac{6}{1}$	$\frac{6}{3}$