Example 115. 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 116. (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 $a^d \equiv 1 \pmod{n}$. □

Example 117. 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 $3^{4242} \equiv 3^2 = 9 \pmod{100}$.

Example 118. Compute $7^{100} \pmod{60}$.

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 $100 \equiv 4 \pmod{16}$, we have $7^{100} \equiv 7^4 \pmod{60}$.

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

13 Multiplicative order and primitive roots

Example 119. (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 120. 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 121. 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 122. 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.