Example 111. What are the last two (decimal) digits of 3^{4242}?

Solution. We need to determine $3^{4242} \pmod{100}$. $\phi(100) = \phi(2^2 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

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 112. Show that $a^{100} \equiv a^4 \pmod{60}$ for any integer a.

First attempt. Since $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = 60\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 16$, Euler's theorem shows that $a^{16} \equiv 1 \pmod{60}$ provided that $\gcd(a, 60) = 1$. Since $100 \equiv 4 \pmod{16}$, it follows that, for those a, we indeed have $a^{100} \equiv a^4 \pmod{60}$.

Brute force. Not that, if everything else fails, we can always establish this congruence by checking all 60 residue classes for a modulo 60 (better: only those not yet covered by Euler's theorem).

Solution. By the Chinese remainder theorem, since $60 = 2^2 \cdot 3 \cdot 5$, this is true if and only if

$$\begin{aligned} a^{100} &\equiv a^4 \pmod{4} \\ a^{100} &\equiv a^4 \pmod{3} \\ a^{100} &\equiv a^4 \pmod{5} \end{aligned}$$

for all integers a. But each of these three congruences is easy to check!

Modulo 3 and 5 this follows from Fermat's little theorem (for instance, modulo 5, we have $a^4 \equiv 1 \pmod{5}$ if $5 \nmid a$, so that both a^{100} and a^4 are congruent to 1; if, on the other hand, $5|a$ then both a^{100} and a^4 are congruent to 0 modulo 5).

Similarly, Euler's theorem shows that $a^{100} \equiv a^4 \pmod{4}$ provided that $\gcd(a, 4) = 1$. Otherwise, that is $2|a$, or, equivalently, $a \equiv 0 \pmod{4}$ or $a \equiv 2 \pmod{4}$. In both of these cases, a^{100} and a^4 are each congruent to 0 modulo 4.

Important comment. The lesson to learn is that, whenever we deal with congruences modulo composite numbers, we should consider applying the Chinese remainder theorem.

Advanced comment. In general, for any positive n, we have $a^n \equiv a^{n - \phi(n)} \pmod{n}$ for all integers a. This generalizes the congruence $a^p \equiv a \pmod{p}$, where p is a prime but a can be any integer. It isn't quite strong enough to directly solve our problem at hand.

Example 113. Fermat's little theorem can be stated in the slightly stronger form:

n is a prime if and only if $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \{1, 2, \ldots, n-1\}$.

Why? Fermat's little theorem covers the "if" part. The "only if" part is a direct consequence of the fact that, if n is composite with divisor d, then $d^{n-1} \not\equiv 1 \pmod{n}$. (Why?!)

Fermat primality test

Input: number n and parameter k indicating the number of tests to run

Output: "not prime" or "possibly prime"

Algorithm:

Repeat k times:
  Pick a random number a from $\{2, 3, \ldots, n-2\}$.
  If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "possibly prime".

Armin Straub
straub@southalabama.edu

However. Not usually used in practice because of the existence of absolute pseudoprimes, which are discussed below: although rare, for these numbers, the Fermat primality test is essentially just a random search for factors of n. There do exist, however, extensions of the Fermat primality test which solve these issues.

[For instance, Miller-Rabin, which checks whether $a^{n-1} \equiv 1 \pmod{n}$ but also checks whether values like $a^{(n-1)/2}$ are congruent to ± 1.]

Advanced comment. If n is composite but not an absolute pseudoprime, then at least half of the values for a satisfy $a^{n-1} \not\equiv 1 \pmod{n}$ and so reveal that n is not a prime.

Example 114. Suppose we want to determine whether $n = 221$ is a prime.

First, maybe we pick $a = 38$ randomly from $\{2, 3, \ldots, 219\}$.

We then calculate that $38^{220} \equiv 1 \pmod{221}$. So far, 221 is behaving like a prime.

Next, we might pick $a = 24$ randomly from $\{2, 3, \ldots, 219\}$.

We then calculate that $24^{220} \equiv 81 \not\equiv 1 \pmod{221}$.

We therefore stop and have determined that 221 is not a prime.

Important comment. We have done so without finding a factor of n!

Comment. Since 38 was giving us a false impression regarding the primality of n, it is called a **Fermat liar**.

On the other hand, we say that 221 is a **pseudoprime** to the base 38.

Comment. In this example, we were actually unlucky that our first "random" pick was a Fermat liar: only 14 of the 218 numbers (about 6.4%) are liars.

Definition 115. Given $a > 1$. A composite number n such that $a^n \equiv a \pmod{n}$ is called a **pseudoprime** to the base a.

The smallest pseudoprimes to the base 2 are $341, 561, 645, 1105, 1387, 1729, \ldots$. There are infinitely many of these, but they are much rarer than primes! (Only 247 of these up to 10^6, compared to $78,498$ primes.)

Example 116. Somewhat suprisingly, there exist numbers which are pseudoprime to any base. These are called **absolute pseudoprimes** or Carmichael numbers.

The first few are $561, 1105, 1729, 2465, \ldots$ (it was only shown in 1994 that there are infinitely many of them). These are very rare, however: there are 43 absolute pseudoprimes less than 10^6. (Versus $78,498$ primes.)

Example 117. (homework)

- Show that 25 is a pseudoprime to base 7.
- Show that $561 = 3 \cdot 11 \cdot 17$ is an absolute pseudoprime.

  Hint. Proceed using the Chinese remainder theorem, as in the second example today.

Armin Straub
straub@southalabama.edu