Review. Fermat's little theorem, and its proof

Example 106. 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 is $1782^{12} \approx 1.025 \cdot 10^{39}$ 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 a lot 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

Theorem 107. (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,

$$a, 2a, 3a, ..., (p-1)a$$

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 $1, 2, ..., p-1$ modulo p. Thus,

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

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

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

$$am_1, am_2, am_3, ..., am_d$$

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 $m_1, m_2, ..., m_d$ modulo n. Thus,

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

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

14 Primality testing

Recall that it is extremely difficult to factor large integers (this is the starting point for many cryptosystems). Surprisingly, it is much simpler to tell if a number is prime.

Example 108. The following is the number from the first lecture, for which RSA Laboratories, until 2007, offered $100,000 to the first one to factorize it. To this day, nobody has been able to do so.

Has the thought crossed your mind that the challengers might be tricking everybody by chosing M to be a huge prime that cannot be factored further? Well, we'll talk more about primality testing soon. But we can actually quickly convince ourselves that M cannot be a prime. If M was prime then, by Fermat's little theorem, $2^{M-1} \equiv 1 \pmod{M}$. Below, we compute $2^{M-1} \pmod{M}$ and find that $2^{M-1} \not\equiv 1 \pmod{M}$. This proves that M is not a prime. It doesn't bring us any closer to factoring it though.

Comment. Ponder this for a while. We can tell that a number is composite without finding its factors. Both sides to this story (first, being able to efficiently tell whether a number is prime, and second, not being able to factor large numbers) are of vital importance to modern cryptography.

```
Sage] rsa = Integer("135066410865995223349603216278805969938881475605667027524485143851\
                    526510604859533833940287150571909441798207282164471551373680419703\
                    964191743046496589274256239341020864383202110372958725762358509643\
                    110564073501508187510676594629205563685529475213500852879416377328\
                    533906109750544334999811150056977236890927563")

Sage] power_mod(2, rsa-1, rsa)

    1209390944320336158676505953529569968675400984635889512389028083675567339322020593385 3\
    348534147116662841968124107288512373904071077139405352848835710498409193003137847878955\
    226029615123284879513798127406300472693925500331497519103479951096634123177725212482975\
    950196643140069546889855131459759160570963857373851
```

Comment. Just for giggles, let us emphasize once more the need to compute $2^{N-1} \pmod{N}$ without actually computing 2^{N-1}. Take, for instance, the 1024 bit RSA challenge number $N = 135...563$ in this example. The number 2^{N-1} itself has $N - 1 \approx 2^{1024} \approx 10^{308.3}$ binary digits. It is often quoted that the number of particles in the visible universe is estimated to be between 10^{80} and 10^{100}. Whatever these estimates are worth, our number has WAY more digits (!) than that. Good luck writing it out! [Of course, the binary digits are a single 1 followed by all zeros. However, we need to further compute with that!]

Comment. There is nothing special about 2. You could just as well use, say, 3.

Example 109. Fermat's little theorem can be stated in the slightly stronger form:

n is a prime $\iff$ $a^{n-1} \equiv 1 \pmod{n}$ for all $a \in \{1, 2, ..., n-1\}$

Why? Fermat's little theorem covers the "$\Longrightarrow$" part. The "$\Longleftarrow$" 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?!)

Review. In the second part, we used that the **contrapositive** of $A \Longrightarrow B$ is the logically equivalent statement $\neg B \Longrightarrow \neg A$.

Fermat primality test

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

Output: "not prime" or "likely prime"

Algorithm:

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

If $a^{n-1} \equiv 1 \pmod{n}$ although n is composite, then a is often called a **Fermat liar**.

On the other hand, if $a^{n-1} \not\equiv 1 \pmod{n}$, then n is composite and a is called a **Fermat witness**.

Flaw. There exist certain composite numbers n (see Example 111) for which every a is a Fermat liar (or reveals a factor of n). For this reason, the Fermat primality test should not be used as a general test for primality. That being said, for very large random numbers, it is exceedingly unlikely to meet one of these troublesome numbers, and so the Fermat test is indeed used for the purpose of randomly generating huge primes (for instance in PGP). In fact, in that case, we can even always choose $a=2$ and $k=1$ with virtual certainty of not messing up.

There do exist 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 (see Example 111), 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. This is more of a theoretical result: for most large composite n, almost every a (not just half) will be a Fermat witness.

Example 110. Suppose we want to determine whether $n=221$ is a prime. Simulate the Fermat primality test for the choices $a=38$ and $a=24$.

Solution.

- First, maybe we pick $a=38$ randomly from $\{2, 3, ..., 219\}$.
  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 $\{2, 3, ..., 219\}$.
  We then calculate that $24^{220} \equiv 81 \not\equiv 1 \pmod{221}$. We stop and conclude that 221 is not a prime.

Important comment. We have done so without finding a factor of n. (To wit, $221 = 13 \cdot 17$.)

Comment. Since 38 was giving us a false impression regarding the primality of n, it is called a **Fermat liar** modulo 221. Similarly, we say that 221 is a **pseudoprime** to the base 38.

On the other hand, we say that 24 was a **Fermat witness** modulo 221.

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. As indicated above, for most large composite numbers, the proportion of liars will be exceedingly small.

Example 111. Somewhat suprisingly, there exist composite numbers n with the following disturbing property: every residue a is a Fermat liar or $\gcd(a, n) > 1$.

This means that the Fermat primality test is unable to distinguish n from a prime, unless the randomly picked number a happens to reveal a factor (namely, $\gcd(a, n)$) of n (which is exceedingly unlikely for large numbers).

[Recall that, for large numbers, we do not know how to find factors even if that was our primary goal.]

Such numbers are called **absolute pseudoprimes** or Carmichael numbers.

The first few are $561, 1105, 1729, 2465, ...$ (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.)