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 91. The following is the number from Example 89, for which RSA Laboratories, until 2007, offered $100,000 to the first one to factorize it. Nobody has been able to do so to this day.

Has the thought crossed your mind that the challengers might be tricking everybody by choosing 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\
                     525510604859533833940287150571909441798207282164471551373680419703\
                     964191743046496589274256239341020864383202110372958725762358509643\
                     110564073501508187510676594629205563685529475213500852879416377328\
                     533906109750544334999811150056977236890927563")

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

    120939094432033615867650595352956996867540098463588951238902808367556733932202059338 53\
    348534147116662841968124107288512373904071077139405352848835710498409193003137847878 95\
    226029615123284879513798127406300472693925500331497519103479951096634123177725212482 97\
    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 Example 91, we computed $2^{N-1} \pmod{N}$, observed that it was $\not\equiv 1$ and concluded that N is not prime. The number 2^{N-1} itself has $N \approx 2^{1024} \approx 10^{308.3}$ 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 92. (bonus challenge) Find the factors of the following number $M = pq$:

89320280057437363393608386387469360495079915773073599087435569428108 27\
07615146116506918133536640188765047775335776026093439165454319252186 33\
75114106509563452970373049082933244013107347141654282924032714311

As indicated in Example 89, this is difficult. Through some sort of espionage, however, you have learned that $\phi(M)$ is:

89320280057437363393608386387469360495079915773073599087435569428108 27\
07615146116506918133536640188675726495278338662699830779066849891691 25\
75956375773572578614678768000225628866990840223520746283867797512

In general, if $M = pq$ is a product of two large primes p, q, given $\phi(M)$, how can we factor M?

Send me the factorization, and an explanation how you found it, by next week for a bonus point!

Comment. Even if we don't know the number of prime factors of M (in the above case we know that M is a product of two primes), we can "efficiently" factor M if we know the value of $\phi(M)$.

Armin Straub
straub@southalabama.edu

Example 93. 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?!)

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 called a **Fermat liar** modulo n.

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

Flaw. There exist certain composite numbers n (see Definition 97) 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.

Next class, we will discuss an extension of the Fermat primality test which solves these issues (and is just mildly slower).

Advanced comment. If n is composite but not an absolute pseudoprime (see Definition 97), 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 94. 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 95. Which of $6, 7, 8, 9$ are Fermat liars modulo 25?

Solution. Recall that a is a Fermat liar modulo 25 if $a^{24} \equiv 1 \pmod{25}$. We compute $6^{24} \equiv 21$, $7^{24} \equiv 1$, $8^{24} \equiv 21$, $9^{24} \equiv 11$ (all modulo 25). It follows that, among those four, only 7 is a Fermat liar modulo 25.

Example 96. Which of $10, 15, 20, 25, 30$ are pseudoprimes to the base 7?

Solution. Recall that n is a pseudoprime to the base 7 if $7^{n-1} \equiv 1 \pmod{n}$. We compute $7^9 \equiv 7 \pmod{10}$, $7^{14} \equiv 4 \pmod{15}$, $7^{19} \equiv 3 \pmod{20}$, $7^{24} \equiv 1 \pmod{25}$, $7^{29} \equiv 7 \pmod{30}$. It follows that, among those five, only 25 is a pseudoprime to the base 7.

Absolute pseudoprimes

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:

Definition 97. A composite positive integer n is an **absolute pseudoprime** (or Carmichael number) if $a^{n-1} \equiv 1 \pmod{n}$ holds for each integer a with $\gcd(a, n) = 1$.

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 98. Show that 561 is an absolute pseudoprime.

Solution. We need to show that $a^{560} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561.

Since $561 = 3 \cdot 11 \cdot 17$, $a^{560} \equiv 1 \pmod{561}$ is eqivalent to $a^{560} \equiv 1 \pmod{p}$ for each of $p = 3, 11, 17$.

By Fermat's little theorem, we have $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$. Since $2, 10, 16$ each divide 560, it follows that indeed $a^{560} \equiv 1 \pmod{p}$ for $p = 3, 11, 17$.

Comment. Korselt's criterion (1899) states that what we just observed in fact characterizes absolute pseudoprimes. Namely, a composite number n is an absolute pseudoprime if and only if n is squarefree, and for all primes p dividing n, we also have $p - 1 | n - 1$.

Comment. Our argument above shows that, in fact, $a^{80} \equiv 1 \pmod{561}$ for all invertible residues a modulo 561.

Theorem 99. (Korselt's Criterion) A composite positive integer n is an absolute pseudoprime if and only if n is squarefree and $(p-1)|(n-1)$ for each prime divisor p of n.

Proof. Here, we will only consider the "if" part (the "only if" part is also not hard to show but the typical proof requires a little more insight into primitive roots than we currently have).

To that end, assume that n is **squarefree** and that $(p-1)|(n-1)$ for each prime divisor p of n. Let a be any integer with $\gcd(a, n) = 1$. We will show that $a^{n-1} \equiv 1 \pmod{n}$.

n being squarefree means that its prime factorization is of the form $n = p_1 \cdot p_2 \cdots p_d$ for distinct primes p_i (this is equivalent to saying that there is no integer $m > 1$ such that $m^2 | n$). By Fermat's little theorem $a^{p_i - 1} \equiv 1 \pmod{p_i}$ and, since $(p_i - 1)|(n-1)$, we have $a^{n-1} \equiv 1 \pmod{p_i}$ for all p_i. It therefore follows from the Chinese remainder theorem that $a^{n-1} \equiv 1 \pmod{n}$. □

Comment. Modulo a prime p, Fermat's little theorem implies that $a^p \equiv a \pmod{p}$ for each integer a. (Why?!) It therefore follows from the above argument that, for an absolute pseudoprime n, we have $a^n \equiv a \pmod{n}$ for each integer a (and this property characterizes absolute pseudoprimes).