Pseudoprimes

According to Fermat's little theorem, if n is prime and $b \in \mathbb{Z}$, then

$$b^n \equiv b \pmod{n}.$$

The contrapositive of this statement says that

"if $b^n \not\equiv b \pmod{n}$ for some integer b, then n is composite.".

This is true (why?)

How about the converse of Fermat's little theorem? It is not always true. In other words, there are composite numbers n such that $b^n \equiv b \pmod{n}$ is true for some $b \in \mathbb{Z}$.

ex: Let $n = 341 = 11 \cdot 31$.

By FLT (Fermat's Little Theorem),

$$2^{10} \equiv 1 \pmod{11}$$

$$\therefore\ 2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$$

Also, $2^{340} = (2^5)^{68} = (32)^{68} \equiv 1 \pmod{31}$

$\therefore$ by Corollary 4.9.1

$$2^{340} \equiv 1 \pmod{11 \cdot 31}$$

$$\Rightarrow \quad 2^{340} \equiv 1 \pmod{341}$$

$$\Rightarrow \quad 2^{341} \equiv 2 \pmod{341}$$

but 341 is not prime.

Definition: Let $b \in \mathbb{Z}^{+}$ and n be a composite positive integer. If $b^{n} \equiv b \pmod{n}$ then n is called a pseudoprime to base b.

Note that, if $\gcd(b, n) = 1$, then we get (by Corollary 4.5.1)

$$b^{n-1} \equiv 1 \pmod{n}.$$

ex: 341 is a pseudoprime to base 2 (as seen in the above example).

$561 = 3 \cdot 11 \cdot 17$ is a pseudoprime as

$$2^{560} \equiv 1 \pmod{561}$$

and 645 is a pseudoprime as

$$2^{644} \equiv 1 \pmod{645}.$$

There are infinitely many pseudoprimes to any base b. We wish to prove it for $b = 2$. First, a lemma.

Lemma 6.1: Let $d, n \in \mathbb{Z}^+$.

If $d \mid n$, then $(2^d - 1) \mid (2^n - 1)$.

Proof: exercise

Theorem: There are infinitely many pseudoprimes to base 2.

Proof: We'll show that if n is an odd pseudoprime to base 2, then $m = 2^n - 1$ is also a pseudoprime to base 2.

We already have a pseudoprime to base 2, which is 341. (Therefore, once we prove this theorem, we can say that $2^{341} - 1$ is also a pseudoprime.)

Thus, we can find an increasing sequence of pseudoprimes $n_1, n_2, n_3, \ldots$ such that

$$n_{k+1} = 2^{n_k} - 1 \quad \forall\, k = 1, 2, 3, \ldots$$

with $n_1 = 341$.

Okay, let's start!

Let n be an odd pseudoprime to base 2.

Then, n is composite and

$$2^{n-1} \equiv 1 \pmod{n}.$$

Then, $n = dt$ for some $d, t \in \mathbb{Z}$ with

$1 < d, t < n.$

We proceed to show that $m = 2^n - 1$ is a pseudoprime. For this, we need to show that m is composite, and that $2^{m-1} \equiv 1 \pmod{m}$.

First, let's prove that m is composite.

Since $d \mid n$, by Lemma 6.1, we've

$$(2^d - 1) \mid (2^n - 1).$$

Also, $1 < d < n$, so $1 < 2^d - 1 < 2^n - 1.$

$\therefore$ $2^n - 1 \; (= m)$ is composite.

Next, let's prove that $2^{m-1} \equiv 1 \pmod{m}$.

We've
$$2^{n-1} \equiv 1 \pmod{n}$$
$$\Rightarrow 2^n \equiv 2 \pmod{n}.$$
$$\therefore 2^n - 2 = kn \text{ for some } k \in \mathbb{Z}.$$

$$\therefore 2^{m-1} = 2^{(2^n - 1) - 1} = 2^{2^n - 2} = 2^{kn}$$

$$\therefore 2^{m-1} - 1 = 2^{kn} - 1$$

Now, $2^n - 1$ divides $2^{kn} - 1$ (by Lemma 6.1 as $n \mid (kn)$)

$\therefore$ $2^n - 1$ divides $2^{m-1} - 1$.

$\therefore$ $m \mid (2^{m-1} - 1)$ $\quad (\because m = 2^n - 1)$

$\therefore$ $2^{m-1} \equiv 1 \pmod{m}$

Hence, m is a pseudoprime to base 2.

If we can show that $2^{n-1} \equiv 1 \pmod{n}$ and that $b^{n-1} \not\equiv 1 \pmod{n}$ for some integer b, then it follows that n is composite, hence n is a pseudoprime to base 2.

ex: We know 341 is a pseudoprime to base 2. Let's check whether it's pseudoprime to base 7.

$$7^3 = 343 \equiv 2 \pmod{341}$$

$$2^{10} = 1024 \equiv 1 \pmod{341}$$

$$\therefore\ 7^{340} = (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7$$

$$\equiv (2^{10})^{11} \cdot 2^3 \cdot 7$$

$$\equiv 2^3 \cdot 7 \equiv 56 \not\equiv 1 \pmod{341}$$

$\therefore$ 341 is not a pseudoprime to base 7. Moreover, by the contrapositive of Fermat's little theorem, 341 is composite.

Carmichael Numbers

There are composite integers that satisfy the condition

$b^{n-1} \equiv 1 \pmod{n}$ for all b with $\gcd(b,n)=1$.

In other words, n is a pseudoprime to each b that satisfy $\gcd(b,n)=1$. Such integers are called Carmichael numbers or absolute pseudoprimes.

ex: Let's show that 561 is a Carmichael number.

$$561 = 3 \cdot 11 \cdot 17$$

Let b be s.t. $\gcd(b, 561) = 1$.
Then, it follows that

$$\gcd(b,3) = \gcd(b,11) = \gcd(b,17) = 1.$$

Then, from Fermat's little theorem, we've

$$b^2 \equiv 1 \pmod{3}$$
$$b^{10} \equiv 1 \pmod{11}$$
$$b^{16} \equiv 1 \pmod{17}$$

$$\therefore\ b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$$
$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$$
$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$$

Then, by Corollary 4.9.1,

$$b^{560} \equiv 1 \pmod{561}$$

Hence $$b^{560} \equiv 1 \pmod{561}$$

for all b with $\gcd(b, 561) = 1$.

Carmichael conjectured, in 1912, that there are infinitely many Carmichael numbers. It was proved by Alford, Granville, and Pomerance in 1992, after 80 years.