Fermat’s Little Theorem

A number of results from elementary number theory are useful for solving contest-type problems. A standard theorem is Fermat’s Little Theorem If \( p \) is a prime and \( a \) is a positive integer, then

\[
a^p \equiv a \pmod{p}.
\]

If \( a \) is an integer not divisible by \( p \), then

\[
a^{p-1} \equiv 1 \pmod{p}.
\]

We can see this in action for \( p = 7 \) below, where all numbers are calculated modulo 7. Notice that both versions are illuminated by the last two columns.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a^2 )</th>
<th>( a^3 )</th>
<th>( a^4 )</th>
<th>( a^5 )</th>
<th>( a^6 )</th>
<th>( a^7 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

Now let’s use this theorem in a problem. In the seventh season episode *Treehouse of Horror VI* of *The Simpsons* (first aired October 30 1995), during the segment *Homer 3D*, dim witted protagonist Homer Simpson is transported into three dimensional space. While there, he encounters a number of mathematical objects, like geometric solids and the coordinate axes, as well as a number of equations that float by. One of the equations states

\[
1782^{12} + 1841^{12} = 1922^{12},
\]

which violates Fermat’s Last Theorem (which had just been proved two years prior to this episode airing after being unsolved for more than 350 years!). The example
is large enough that it will probably fool your calculator. My calculator, with a
10 digit display, has $1782^{12} + 1841^{12}$ and $1922^{12}$ agreeing to all displayed digits as
does $1922^{12} - 1841^{12}$ and $1782^{12}$. Warning lights might have gone on if I calculated
$1922^{12} - 1782^{12}$ and $1841^{12}$ and noticed that they differed in the last decimal place.
Yet, my calculator gives the following results:

$$ \sqrt[12]{1782^{12} + 1841^{12}} = 1922, $$
$$ \sqrt[12]{1922^{12} - 1841^{12}} = 1782, $$
$$ \sqrt[12]{1922^{12} - 1782^{12}} = 1841. $$

Although computer algebra software like Maple and Mathematica would make
short work of this problem, since none of $1782$, $1841$ and $1922$ is a multiple of 13,
we can apply Fermat’s theorem to note that

$$ 1782^{12} + 1841^{12} \equiv 1 + 1 \not\equiv 1 \equiv 1922^{12} \pmod{13}, $$

Thus the equation is false.

Many proofs of Fermat’s Little Theorem exist; my favourite uses properties
of modular arithmetic. Consider the set $\{1, 2, 3, \ldots, p-1\}$, and let $a$ be a positive
integer with $1 \leq a < p$; then if we reduce the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ modulo $p$,
it is just a permutation of the original set. This is true since no element of the new
set is divisible by $p$ since all factors in the products are less than $p$. Similarly, there
are no duplications in the set, since if $am \equiv an \pmod{p}$, then $m \equiv n \pmod{p}$.
Thus

$$ (a)(2a)(3a) \cdots ((p-1)a) \equiv (1)(2)(3) \cdots (p-1) \pmod{p} $$
$$ \Rightarrow a^{p-1}(1)(2)(3) \cdots (p-1) \equiv (1)(2)(3) \cdots (p-1) \pmod{p} $$
$$ \Rightarrow a^{p-1} \equiv 1 \pmod{p} $$

It is important to note that the converse of Fermat’s little theorem is false.
That is, if $a^{n-1} \equiv 1 \pmod{n}$ it doesn’t mean that $n$ is prime. A number $n$ that
satisfies $a^{n-1} \equiv 1 \pmod{n}$, for some positive integer $a$, yet is not prime, is called
a pseudoprime in base $a$. An example would be $n = 341 = 11 \times 31$ which is a pseudoprime base 2. There even exist extremal pseudoprimes, that is, numbers
$n$ that are pseudoprime to all bases $a$ that are relatively prime to them. That
is, $n$ satisfies $a^{n-1} \equiv 1 \pmod{n}$ for every positive integer $a$, $1 < a < n$, such
that gcd($a, n$) = 1. These numbers are called Carmichael numbers, the smallest
of which is $561 = 3 \times 11 \times 17$.

Try your hand with the following problems.

Problems:

1. Can you spot a much easier proof that $1782^{12} + 1841^{12} \neq 1922^{12}$? After
   finding it, feel free to slap yourself in the head and say “D’oh!”
   You can check out other examples of mathematics in The Simpsons at [2].

\textit{Crux Mathematicorum}, Vol. 38(6), June 2012
2. In the season 10 episode *The Wizard of Evergreen Terrace* of *The Simpsons* that first aired September 20, 1998, Homer is seen writing on a chalkboard which contains the equation $3987^{12} + 4365^{12} = 4472^{12}$ (along with a demonstration of how to transform a torus into a sphere). Show that, once again, this equation is incorrect. You can check out other examples of “Fermat near misses” at [1].

3. Show that 341 is a pseudoprime base 2.

4. Pick several values of $a$, with $1 < a < 561$ and $\gcd(561, a) = 1$ and show that 561 is a pseudoprime base $a$. You can check out pseudoprimed, Carmichael numbers and everything prime at [3].

5. Prove that $n^{20} - 1$ is divisible by 11 for all positive integers relatively prime to 11.

6. Show that 129 is **not** prime using Fermat’s little theorem. **Hint:** Evaluate $2^{128} \pmod{129}$.

References

