More along Fermat’s little theorem

We have seen that $a^{p-1} \equiv 1 \pmod{p}$ when $\gcd(a, p) = 1$. How about mod $n$ for a general positive integer $n$? To extend from case of prime numbers, a reasonable case, as we see in Q1 in Problem Set 1, will be that of prime powers.

**Theorem 3.1.** Let $p$ be a prime and $s \geq 1$. For any $a$ with $\gcd(a, p) = 1$ we have

$$a^{(p-1)p^s-1} \equiv 1 \pmod{p^s}$$

*First proof.* When $s = 1$, this is just Fermat’s little theorem. We use induction on $s$. For $s \geq 2$, to see that $p^s | a^{(p-1)p^s-1} - 1$, let $x = a^{(p-1)p^{s-2}}$. By the induction hypothesis we have $p^{s-1} | x - 1$. Then Q1(a) of Problem Set 1 gives $p^s | x^p - 1 = a^{(p-1)p^{s-1}} - 1$, which is what we want.

In fact, let me give a slightly different proof of Q1(a) than hinted. Suppose $x \equiv 1 \pmod{p^{s-1}}$, so that $x = 1 + p^{s-1}y$. Then $x^p = (1 + p^{s-1}y)^p = 1 + \binom{p}{1}p^{s-1}y + \binom{p}{2}p^{2s-2}y^2 + \ldots$.

Since $s \geq 2$, one notes that all terms except the 1 is divisible by $p^s$. Thus $x^p \equiv 1 \pmod{p^s}$.

One however notes that, when either $p \geq 3$, or $s \geq 3$, from the second term onwards they are all divisible by $p^{s+1}$. Suppose $\gcd(y, p) = 1$. Then $\binom{p}{s}p^{s-1}y$ is not divisible by $p^{s+1}$ yet all terms after it are. In this case we have $p^{s+1} \nmid x^p - 1$.

**Definition 3.2.** Write $p^t \| n$ if $p^t | n$ but $p^{t+1} \nmid n$.

**Lemma 3.3.** Suppose $p^{s-1} \| x - 1$ where $s \geq 2$. If either $p \geq 3$ or $s \geq 3$, then $p^s \| x^p - 1$.

**Example 3.4.** We had $7^1 \| 10^6 - 1$. This implies $7^s \| 10^{6\cdot 7^{s-1}} - 1$ (we use that $p \geq 3$ in the lemma). This refines the result in Q1(b) of Problem Set 1 that $6 \cdot 7^{s-1}$ is the minimal period of the decimal expression of $1/7^s$.

**Problem 3.5.** Find all positive integers $n$ such that

$$\frac{2^n + 1}{n^2}$$

is an integer.

*Second proof of Theorem 3.1.* Consider the set of integers from 1 and $p^s$ that are coprime to $p^s$, i.e. coprime to $p$. Exactly $p^{s-1}$ of them are NOT coprime to $p$ (i.e. divisible by $p$), and thus the rest $(p - 1) \cdot p^{s-1}$ are coprime to $p$. Let $X$ be the set of these numbers, and

$$m := \prod_{x \in X} x$$

1
be the product of them. Now consider
\[ a^{(p-1)p^{s-1}m} = \prod_{x \in X} ax \]

We again have that for \( x_1, x_2 \in X \), \( ax_1 \equiv ax_2 \pmod{p^s} \) only if \( x_1 = x_2 \). This is because if \( p^s \mid a(x_1 - x_2) \), then \( p^s \mid x_1 - x_2 \) by the unique factorization theorem and the assumption that \( \gcd(a, p) = 1 \). Thus we see that elements of the form \( ax, x \in X \) are congruent modulo \( p^s \) to those in \( X \), in a bijective manner. Thus we have
\[ a^{(p-1)p^{s-1}m} \equiv m \pmod{p^s} \]
from which
\[ a^{(p-1)p^{s-1}} \equiv 1 \pmod{p^s} \]
follows as \( m \) is also coprime to \( p \).

\[ \square \]