$a^n \pm 1$

Yufei Zhao
Trinity College, Cambridge

yufei.zhao@gmail.com

April 2011

In this lecture we look at some problems involving expressions of the form $a^n \pm 1$. Let's start with a couple of warm up problems.

Problem. Let a, m, n be positive integers. Prove that $\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1$.

Solution. Using the identity $\frac{x^k-1}{x-1} = x^{k-1} + \cdots + x + 1$, we know that $a^e - 1 \mid a^d - 1$ whenever $e \mid d$, so $a^{\gcd(m,n)-1}$ divides both $a^n - 1$, and $a^m - 1$. On the other hand, if r divides both $a^n - 1$ and $a^m - 1$, then r must be relatively prime to a, so a can be inverted mod r. There exists integers s, t such that $sn + tm = \gcd(m, n)$. So

$$a^{\gcd(m,n)} \equiv a^{sn+tm} \equiv (a^n)^s (a^m)^t \equiv 1 \pmod r.$$

Any common divisor of $a^n - 1$ and $a^m - 1$ must be a divisor of $a^{\gcd(m,n)} - 1$ as well. This proves that $\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1$. □

Another approach is to use the Euclidean algorithm. If $m > n$, say, then

$$\gcd(a^n - 1, a^m - 1) = \gcd(a^n - 1, a^m - 1 - a^{m-n}(a^n - 1)) = \gcd(a^n - 1, a^{m-n} - 1).$$

So the the Euclidean algorithm process that gives us $\gcd(n, m) = d$ also gives us $\gcd(a^n - 1, a^m - 1) = a^d - 1$.

For a prime number p and a nonnegative integer k, write $p^k \parallel n$ to mean that $p^k \mid n$ and $p^{k+1} \nmid n$. In this case we say that n is *exactly divisible* by p^k.

Problem. Let k be a nonnegative integer. Prove that $3^{k+1} \parallel 2^{3^k} + 1$.

From Euler's theorem, we know that $3^{k+1} \mid 2^{2\cdot 3^k} - 1 = (2^{3^k} + 1)(2^{3^k} - 1)$. We have $2^{3^k} - 1 \equiv (-1)^{3^k} - 1 \equiv 1 \pmod 3$. So $3^{k+1} \mid 2^{3^k} + 1$. However, this doesn't show us that $3^{k+2} \nmid 2^{3^k} + 1$, so we adopt a different approach.

Solution. We use induction on k. We can check for $k = 0$. Suppose that $k \geq 1$ and $3^k \parallel 2^{3^{k-1}} + 1$. We would like to show $3^{k+1} \parallel 2^{3^k} + 1$. It suffices to show that $(2^{3^k} + 1)/(2^{3^{k-1}} + 1)$ is divisible by 3 but not 9. We can check this by hand when $k = 1$. For $k \geq 2$, we have

$$\frac{2^{3^k} + 1}{2^{3^{k-1}} + 1} = (2^{\cdot 3^{k-1}})^2 - 2^{3^{k-1}} + 1 \equiv (-1)^2 - (-1) + 1 \equiv 3 \pmod{3^k}$$

by the induction hypothesis, and hence it is divisibly by 3 but not 9. □

The previous problem showed us a useful technique, whose idea is captured in the following lemma.

Lemma. *(Exponent lifting trick) Let $a \geq 2, k \geq 1, \ell \geq 0$ be integers, p a prime number. Suppose $(p,k) \neq (2,1)$, and*

$$p^k \parallel a-1 \quad \textit{and} \quad p^\ell \parallel n.$$

Then

$$p^{k+\ell} \parallel a^n - 1.$$

When $n = p^\ell$, we obtain the conclusion that $p^k p^\ell \parallel a^{p^\ell} - 1$, so that p^ℓ is "lifted" into the exponent.

We give two proofs of the lemma. The first proof uses induction following ideas in the previous problem, whereas the second proof does not use induction.

First proof. Write $n = p^\ell m$, where $p \nmid m$. Use induction on ℓ. When $\ell = 0$,

$$a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + a + 1)$$

where

$$a^{m-1} + a^{m-2} + \cdots + a + 1 \equiv 1^{m-1} + 1^{m-2} + \cdots + 1 + 1 = m \pmod{p^k},$$

and hence not divisible by p. Thus $p^k \parallel a^m - 1$. This concludes the base case $\ell = 0$.

For the inductive step, it suffices to show that $p^{k+\ell} \parallel a^n - 1$ implies $p^{k+\ell+1} \parallel a^{np} - 1$. This amounts to showing that $\frac{a^{np}-1}{a^n-1}$ is divisibly by p by not p^2. We have

$$\frac{a^{np}-1}{a^n-1} = a^{n(p-1)} + a^{n(p-2)} + \cdots + a^n + 1 \equiv 1 + 1 + \cdots + 1 + 1 = p \pmod{p^{k+\ell}}.$$

We are done unless $k + \ell = 1$, i.e., $(k,\ell) = (1,0)$, which we deal with separately. Assume $(k,\ell) = (1,0)$. Let $a^m - 1 = pb$ where $p \nmid b$. We would like to show that $p^2 \parallel a^{pm} - 1$. We have

$$a^{pm} - 1 = (1+pb)^p - 1 = p^2 b + \sum_{i=2}^{p} \binom{p}{i} p^i b^i.$$

Since $p \neq 2$ (excluded as $(p,k) \neq (2,1)$), p^3 divides all the terms except for the first term. Therefore $a^{pm} - 1$ is divisible by p^2 but not p^3. $\square$

Second proof. Write $a = p^k b + 1$ where $p \nmid b$. We have

$$a^n - 1 = (p^k b + 1)^n - 1 = np^k b + \sum_{i=2}^{n} \binom{n}{i} p^{ki} b^i.$$

We have $p^{k+\ell} \parallel np^k b$. It suffices to show that $p^{k+\ell+1} \mid \binom{n}{i} p^{ki} b^i$ for each $i \geq 2$. Note that

$$\binom{n}{i} p^{ki} b^i = \frac{n}{i} \binom{n-1}{i-1} p^{ki} b^i = np^k \frac{p^{k(i-1)}}{i} \binom{n-1}{i-1} b^i.$$

This number is always divisible by $p^{k+\ell+1}$ since the exponent of p in $\frac{p^{k(i-1)}}{i}$ is always positive for $i \geq 2$ as $(p,k) \neq (2,1)$. $\square$

Practice problems:

1. A *primitive root* mod n is a number g such that the smallest positive integer k for which $g^k \equiv 1 \mod n$ is $\phi(n)$.

(a) Show that 2 is a primitive root mod 3^n for any $n \geq 1$.

(b) Show that if g is an odd primitive root mod p such that $p^2 \nmid g^{p-1} - 1$, then g is also a primitive root mod p^n and $2p^n$ for any $n \geq 1$.

2. (Cyclotomic polynomials) For a positive integer n, define the polynomial $\Phi_n(x)$ by

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(n,k)=1}} (x - e^{\frac{2\pi i k}{n}}).$$

   (a) Prove the polynomial identity $\prod_{d|n} \Phi_d(x) = x^n - 1$, where the product is taken over all divisors d of n.

   (b) Prove that $\Phi_n(x)$ is an integer polynomial.

   (c) Let m and n be positive integers, and let p be a prime divisor of $\Phi_n(m)$. Prove that either $p \mid n$ or $n \mid p - 1$.

   (d) (Special case of Dirichlet's theorem) Prove that for every positive integer n, there are infinitely many primes p with $p \equiv 1 \pmod{n}$.

3. (IMO 2003) Let p be a prime number. Prove that there exists a prime number q such that for every integer n, $n^p - p$ is not divisible by q.

4. (a) Prove that $\Phi_m(x)$ and $\Phi_n(x)$ are always relatively prime as polynomials for $m \neq n$.

   (b) Show that if for some integer x, $\Phi_m(x)$ and $\Phi_n(x)$ are not relative prime, then m/n is an integer power of a prime.

5. Let $p_1, p_2, \ldots, p_k$ be distinct primes greater than 3. Let $N = 2^{p_1 p_2 \cdots p_k} + 1$.

   (a) (IMO Shortlist 2002) Show that N has at least 4^n divisors.

   (b) Show that N has at least $2^{2^{k-1}}$ divisors. (Hint: use cyclotomic polynomials)

6. (IMO 1990) Determine all positive integers n such that $\dfrac{2^n+1}{n^2}$ is an integer.

7. (IMO 2000) Does there exist a positive integer N which is divisible by exactly 2000 different prime numbers and such that $2^N + 1$ is divisible by N?

8. Let N be a positive integer ending in digits 25, and m a positive integer. Prove that for some positive integer n, the rightmost m digits of 5^n and N agree in parity (i.e., for $1 \leq k \leq m$, the k-th digit from the right in n is odd if and only if the k-th digit from the right in N is odd).

9. (Hensel's lemma) Let

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_2 x^2 + c_1 x + c_0$$

   be a polynomial with integer coefficients. Its derivative f' is a polynomial defined by

$$f'(x) = n c_n x^{n-1} + (n-1) c_{n-1} x^{n-2} + \cdots + 2 c_2 x + c_1.$$

   Suppose that $a \in \mathbb{Z}$ satisfies $p \mid f(a)$ and $p \nmid f'(a)$. Prove that for any integer k, there exists an integer b satisfying $p^k \mid f(b)$ and $p \mid b - a$.