

# $a^n \pm 1$

## Solutions

Yufei Zhao  
Trinity College, Cambridge

yufei.zhao@gmail.com

April 2011

### Practice problems:

1. A *primitive root* mod  $n$  is a number  $g$  such that the smallest positive integer  $k$  for which  $g^k \equiv 1 \pmod{n}$  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  $n \geq 1$ .

**Solution.** (a) Since  $\phi(3^n) = 2 \cdot 3^{n-1}$ , the problem amounts to showing that  $3^n \nmid 2^{3^{n-1}} - 1$  and  $3^n \nmid 2^{2 \cdot 3^{n-2}} - 1$  (when  $n \geq 2$ ). The first claim follows from reduction mod 3, and the second claim follows from the exponent lifting trick, as  $3 \parallel 2^2 - 1$ , so that  $3^{n-1} \parallel 2^{2 \cdot 3^{n-2}} - 1$ .

(b) Since  $\phi(p^n) = \phi(2p^n) = (p-1)p^{n-1}$ , it suffices to show  $p^n \nmid g^{(p-1)p^{n-2}} - 1$  and  $p^n \nmid g^{d p^{n-1}} - 1$  for any divisor  $d$  of  $p-1$  with  $d < p-1$ . The first claim follows from  $p^{n-1} \parallel g^{(p-1)p^{n-2}} - 1$  by the exponent lifting trick as  $p \parallel g^{p-1} - 1$  by assumption, and the second claim follows from the fact that  $p \mid g^m - 1$  if and only if  $(p-1) \mid m$  as  $g$  is a primitive root mod  $p$ .

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  $p \equiv 1 \pmod{n}$ .

**Solution.** (a) The right-hand side polynomial  $x^n - 1$  can be factored as  $\prod_{k=1}^n (x - e^{\frac{2\pi i k}{n}})$ . For  $1 \leq k \leq n$ , each factor  $x - e^{\frac{2\pi i k}{n}}$  appears exactly once in the left hand side (in  $\Phi_d(x)$  for  $d = \frac{n}{\gcd(n,k)}$ ) and all factors in the left hand side are of this form.

(b) Use induction on  $d$ . We have  $\Phi_1(x) = x - 1$ . Suppose  $\Phi_d(x)$  is an integer polynomial for all  $d < n$ . Then by (a)  $\Phi_n(x)$  is the quotient of two monic integer polynomials, and hence it must also be an integer polynomial.

(c) Suppose  $p \nmid n$  and  $n \nmid p-1$ . We have  $p \mid \Phi_n(m) \mid m^n - 1$  by (a). So  $p \nmid m$ , and hence  $p \mid m^{p-1} - 1$  by Fermat's little theorem. Thus  $p \mid m^{\gcd(p-1,n)} - 1$ . Since  $n \nmid p-1$ ,

$\gcd(p-1, n) < n$ . Since  $p \nmid n$ , we know  $p \nmid \frac{n}{\gcd(p-1, n)}$ . Suppose  $p^k \parallel m^{\gcd(p-1, n)} - 1$ . By the exponent lifting trick, we have  $p^k \parallel m^n - 1$ . However, from (a) we know that the polynomial  $\Phi_n(x)$  is a factor of  $\frac{x^n - 1}{x^{\gcd(p-1, n)} - 1}$ . Setting  $x = m$  gives us a contradiction, since on one hand we have  $p \mid \Phi_n(m)$  but on the other hand  $p$  does not divide  $\frac{m^n - 1}{m^{\gcd(p-1, n)} - 1}$  as it is the quotient of two numbers both exactly divisible by  $p^k$ .

(d) It suffices to show that for every positive integer  $n \geq 2$ , there is at least one prime  $p$  with  $p \equiv 1 \pmod{n}$ , since then we can find infinitely many such  $p$  by finding primes  $p_k$  such that  $p_k \equiv 1 \pmod{kn}$  for each  $k \geq 1$ .

For  $n \geq 2$ ,  $|\Phi_n(n)| > 1$ . Let  $p$  be a prime divisor of  $\Phi_n(n)$ . Since  $\Phi_n(n) \mid n^n - 1$  by (a),  $p \nmid n$ , so  $n \mid p - 1$  by part (b). This gives us the desired prime.

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  $q$ .

**Solution.** Let  $q$  be a prime divisor of  $\Phi_p(p) = \frac{p^p - 1}{p - 1} = p^{p-1} + p^{p-2} + \cdots + p + 1$  with  $p^2 \nmid q - 1$  (this must exist since  $\Phi_p(p) \not\equiv 1 \pmod{p^2}$ ). By problem 2,  $p \mid q - 1$ . If  $n^p \equiv p \pmod{q}$ , then  $p^{\frac{q-1}{p}} \equiv n^{q-1} \equiv 1 \pmod{q}$ . We have  $q \mid \gcd(p^{\frac{q-1}{p}} - 1, p^p - 1) = p^{\gcd(\frac{q-1}{p}, p)} - 1$ , which equals to  $p - 1$  since  $p^2 \nmid q - 1$ . However, we cannot simultaneously have  $q \mid p - 1$  and  $p \mid q - 1$ . Thus  $n^p - p$  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.

**Solution.** (a) The zeros of  $\Phi_n(x)$  and  $\Phi_m(x)$  are distinct, since the zeros of  $\Phi_n(x)$  are precisely the primitive  $n$ -th roots of unity. Thus the polynomials are relatively prime.

(b) Suppose some prime  $p$  divides both  $\Phi_m(x)$  and  $\Phi_n(x)$ . By replacing  $x$  by  $x + p$  if necessary, we may assume that  $x > 1$ . Let us deal with the  $p = 2$  case separately. We claim that if  $\Phi_m(x)$  is even then  $m$  must be a power of 2. Indeed, otherwise let  $q$  be an odd prime divisor of  $m$ , and let  $m = qs$ , then by the previous problem,  $\Phi_m(x)$  divides  $\frac{x^m - 1}{x^s - 1} = x^{(q-1)s} + x^{(q-2)s} + \cdots + x^s + 1$ , which is always odd. The  $p = 2$  case follows.

Now assume that  $p > 2$ . By the previous problem,  $p$  divides  $x^m - 1$  and  $x^n - 1$ , and hence  $p \mid x^{\gcd(m, n)} - 1$ . Let  $p^k \parallel x^{\gcd(m, n)} - 1$ . One of  $\frac{m}{\gcd(m, n)}$  and  $\frac{n}{\gcd(m, n)}$  is not divisible by  $p$ , and assume that it is the latter. Then by the exponent lifting trick,  $p^k \parallel x^n - 1$ . If  $\gcd(m, n) < n$ , then  $\Phi_n(x)$  divides  $\frac{x^n - 1}{x^{\gcd(m, n)} - 1}$ , which is not divisible by  $p$  by the above analysis. This contradicts  $p \mid \Phi_n(x)$ . Hence  $\gcd(m, n) = n$ , i.e.,  $n \mid m$ .

We claim that  $\frac{m}{n}$  is a power of  $p$ . If not, then pick some prime  $q$  dividing  $\frac{m}{n}$ . We have  $p \mid \Phi_n(x) \mid x^n - 1 \mid x^{m/q} - 1$ . By the exponent lifting trick, the same power of  $p$  divides both  $x^m - 1$  and  $x^{m/q} - 1$ . But  $\Phi_m(x)$  divides  $\frac{x^m - 1}{x^{m/q} - 1}$ , which contradicts  $p \mid \Phi_m(x)$ . Thus  $\frac{m}{n}$  is a power of  $p$ .

5. Let  $p_1, p_2, \dots, p_k$  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)

**Solution.** (a) Observe that if  $a$  and  $b$  are coprime odd numbers, then  $\gcd(2^a + 1, 2^b + 1) = 3$ , since their gcd must divide  $\gcd(2^{2a} - 1, 2^{2b} - 1) = 2^{\gcd(2a, 2b)} - 1 = 2^2 - 1 = 3$ . Since  $2^{ab} + 1$  is divisible by both  $2^a + 1$  and  $2^b + 1$ , it must also be divisible by  $\frac{1}{3}(2^a + 1)(2^b + 1)$ .

We use induction on  $k$ . When  $k = 1$ ,  $2^{p_1} + 1$  is divisible by 3 and greater than 9, so it must have at least 4 divisors. Let  $a = p_1 \cdots p_{k-1}$  and  $b = p_k$ . Suppose that  $2^a + 1$  has at least  $4^{k-1}$  divisors. Since  $2^a + 1$  is coprime to  $\frac{1}{3}(2^b + 1)$ , the number  $M = \frac{1}{3}(2^a + 1)(2^b + 1)$  must have at least  $2 \cdot 4^{k-1}$  divisors (for each divisor  $d$  of  $2^a + 1$ , we get two divisors  $d$  and  $\frac{1}{3}(2^b + 1)d$  of  $M$ ). Also  $M \mid N$  and  $N = 2^{ab} + 1 > M^2$  (since  $2^{ab} + 1 > 2^{ab} > 2^{2(a+b+1)} > M^2$ ). So  $N$  has at least  $4^k$  divisors (for each divisor  $d$  of  $M$ , we have divisors  $d$  and  $N/d$ ). This completes the induction.

(b) It suffices to show that  $N$  is divisible by at least  $2^{k-1}$  distinct prime. We have

$$N = 2^{p_1 \cdots p_k} + 1 = \frac{2^{2^{p_1 \cdots p_k}} - 1}{2^{p_1 \cdots p_k} - 1} = \frac{\prod_{d \mid 2^{p_1 \cdots p_k}} \Phi_d(x)}{\prod_{d \mid p_1 \cdots p_k} \Phi_d(x)} = \prod_{d \mid p_1 \cdots p_k} \Phi_{2d}(2).$$

Consider the set of divisors  $d$  of  $p_1 \cdots p_k$  with an odd number of prime factors. There are  $2^{k-1}$  such divisors  $d$ , and they provide mutually coprime  $\Phi_d(2)$  by Problem 4. Take one prime divisor from each such  $\Phi_d(2)$  and we get what we want.

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

**Solution.** We claim that the only solutions are  $n = 1, 3$ . Suppose  $n \notin \{1, 3\}$ . Let  $p$  be the smallest prime divisor of  $n$ . Then  $p \mid 2^n + 1$ , so  $p \mid 2^{2n} - 1$ . By Fermat's little theorem, we also have  $p \mid 2^{p-1} - 1$ . Thus  $p \mid 2^{\gcd(p-1, 2n)} - 1$ . Since  $p$  is the smallest prime divisor of  $n$ , we must have  $\gcd(p-1, 2n) = 2$ . So  $p \mid 2^2 - 1$  and hence  $p = 3$ .

Suppose  $3^k \parallel n$ . We have  $3 \parallel 2^2 - 1$ . So by the exponent lifting trick,  $3^{k+1} \parallel 2^{2n} - 1$ . If  $n^2 \mid 2^n + 1$ , then  $3^{2k} \mid 2^{2n} - 1$ . Thus  $2k \leq k + 1$ , hence  $k = 1$ . Thus  $3 \parallel n$ .

Let  $n = 3m$ . Suppose  $m \neq 1$ . Let  $q$  denote the smallest prime divisor of  $m$ . By the same argument as above, we have  $q \mid 2^{\gcd(q-1, 6m)} - 1$ , and  $\gcd(q-1, 6m) \in \{2, 6\}$ , so  $q$  divides either  $2^2 - 1 = 3$  or  $2^6 - 1 = 63 = 7 \cdot 3^2$ . Since  $3 \parallel n$ ,  $q \neq 3$ , so  $q = 7$ . However,  $2^n + 1 = (2^3)^m + 1 \equiv 2 \pmod{7}$ , so 7 cannot divide  $2^n + 1$ , contradiction. This shows that 1 and 3 are the only solutions.

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  $N$ ?

**Solution.** Yes. We will show by induction that for any  $m \geq 1$ , there exists a positive integer  $N$  divisibly by exactly  $m$  different prime numbers such that  $N \mid 2^N + 1$ .

When  $m = 1$ , choose  $N = 3$ .

We will use the following variant of the exponent lifting trick: if  $p$  is an odd prime,  $a \geq 2$ ,  $k, m \geq 1$ ,  $\ell \geq 0$ ,  $n$  odd,  $p^k \parallel a + 1$ , and  $p^\ell \parallel n$ , then  $p^{k+\ell} \parallel a^n + 1$ . This in fact follows from our usual exponent lifting trick, as neither  $a - 1$  nor  $a^n - 1$  are divisible by  $p$  (since  $a \equiv -1 \pmod{p}$  and  $n$  is odd), so the claim follows as  $p^k \parallel a^2 - 1$  implies  $p^{k+\ell} \parallel a^{2n} - 1$ .

Now suppose  $N = p_1^{a_1} \cdots p_m^{a_m}$  satisfies  $N \mid 2^N + 1$ , where  $p_1, \dots, p_m$  are distinct prime and  $a_i \geq 1$ . Suppose  $p_i^{b_i} \parallel 2^N + 1$  for each  $i$ . Write this as  $p_1^{b_1} \cdots p_m^{b_m} \parallel 2^N + 1$ . Then by above variant of the exponent lifting trick, we have  $p_1^{b_1+\ell} p_2^{b_2} \cdots p_m^{b_m} \parallel 2^{N p_1^\ell} + 1$ . For  $\ell$  sufficiently large, we also have  $p_1^{b_1+\ell} p_2^{b_2} \cdots p_m^{b_m} < 2^{N p_1^\ell} + 1$ , so that  $2^{N p_1^\ell} + 1$  has some prime divisor  $p_{k+1}$  distinct from  $p_1, \dots, p_k$ . Then  $N p_1^\ell p_{k+1} \mid 2^{N p_1^\ell p_{k+1}} + 1$ , and hence we can choose  $N' = N p_1^\ell p_{k+1}$  to complete the induction.

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).

**Solution.** We will prove by induction on  $m$  that there exists infinitely many  $n$  that works. This is trivial when  $m = 1, 2$ .

For the inductive step, it suffices to prove the following claim: if  $n \geq m \geq 2$ , then the rightmost  $m$  digits of  $5^n$  and  $5^{n+2^{m-2}}$  agree in parity, but the  $(m+1)$ -th digit from the right differ in parity.

By the exponent lifting trick, we have  $2^m \parallel 5^{2^{m-2}} - 1$  as  $2^2 \parallel 5 - 1$ . It follows that  $5^{2^{m-2}+n} - 5^n$  is divisible by  $10^m$  but not  $2 \cdot 10^m$ . The claim follows.

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  $p \mid b - a$ .

**Solution.** We use induction on  $k$  to find, for each  $k \geq 1$ , an integer  $b_k$ , satisfying  $b_1 = a$  and

$$b_{k+1} \equiv b_k \pmod{p^k}$$

and

$$f(b_k) \equiv 0 \pmod{p^k}.$$

Note that this implies  $b_k \equiv b_1 = a \pmod{p}$ .

When  $k = 1$ , we can just take  $b_1 = a$ . Now assume that  $k > 1$  and  $b_{k-1}$  has already been chosen. Set

$$b_{k+1} = b_k + p^k r$$

for some integer  $r$  to be decided later. We have

$$\begin{aligned} f(b_{k+1}) &= f(b_k + p^k r) = \sum_{j=0}^n c_j (b_k + p^k r)^j \\ &\equiv \sum_{j=0}^k c_j (b_k^j + j p^k r b_k^{j-1}) = f(b_k) + p^k r f'(b_k) \pmod{p^{k+1}}, \end{aligned}$$

where the modulo equivalence comes from binomial expansion. (This is related to the Taylor expansion in calculus:  $f(x + \epsilon) \approx f(x) + \epsilon f'(x)$ .) From the induction hypothesis, we know  $p^k \mid f(b_k)$ . Also  $b_k \equiv a \pmod{p}$ , so  $p \nmid f'(b_k)$ , and hence  $f'(b_k)$  has an inverse mod  $p$ , say  $t \in \mathbb{Z}$ , satisfying  $f'(b_k) t \equiv 1 \pmod{p}$ . Then setting  $r = -\frac{f(b_k) t}{p^k}$ , we have

$$f(b_{k+1}) \equiv f(b_k) - f(b_k) r f'(b_k) = f(b_k) (1 - r f'(b_k)) \equiv 0 \pmod{p^{k+1}}.$$

since  $p^k \mid f(b_k)$  and  $p \mid 1 - r f'(b_k)$ . This completes the induction step.