Number Theory: Exponentials (revised)

Alison Miller

June 29, 2011

Facts of life about exponentials

Theorem 1. *The Euclidean algorithm for finding gcd's – in particular, for any integers a, b, there are integers m and n such that $ma + nb = \gcd(a, b)$.*

Theorem 2. *If a is relatively prime to b, there exists a' such that $aa' \equiv 1 \pmod{b}$.*

Corollary 1. *If c is relatively prime to m and $ab \equiv ac \pmod{m}$, then $b \equiv c \pmod{m}$.*

Theorem 3. *Let a, n, m be positive integers with $a \geq 2$. Then*

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

The Euler phi function is $\phi(n)$ =the number of integers less than n relatively prime to n. If $n = p_1^{a_1} \cdots p_i^{a_i}$, then $\phi(n)$ is given by the explict formula $\phi(n) = (p_1 - 1)p_1^{a_1 - 1} \cdots (p_i - 1)p_i^{a_i - 1}$

Theorem 4 (Euler's Theorem)**.** *If $\gcd(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

In particular if $m = p$ is prime, we have Fermat's Little Theorem: $a^{p-1} = 1 \pmod{p}$.

Theorem 5. *If $(a, m) = 1$, define $\operatorname{ord}_m(a)$ to be the least j such that $a^j \equiv 1 \pmod{n}$. Then $\operatorname{ord}_m(a)$ divides k if and only if $a^k \equiv 1 \pmod{n}$.*

Combining the two above facts, we conclude that $\operatorname{ord}_m(a)$ divides $\phi(m)$.

Theorem 6 (Partial Converse of Fermat's Little Theorem)**.** *If there is an a for which $a^{m-1} \equiv 1 \pmod{m}$, but for no prime divisor p of $m - 1$ does $a^{\frac{m-1}{p}} \equiv 1 \pmod{m}$, then m is prime.*

Notation: Let $\mathbb{Z}/p\mathbb{Z}$ be the integers mod p.

Theorem 7. *A polynomial of degree n with coefficients in $\mathbb{Z}/p\mathbb{Z}$ has at most n roots in $\mathbb{Z}/p\mathbb{Z}$. (Unlike in the complex numbers, it may have fewer than n roots even when you count multiplicity.)*

Proof. Like in the real numbers; by induction. $\square$

Primitive Roots mod p

Theorem 8 (Existence of a Primitive Root mod p). *For any prime p there exists an element a such that $\operatorname{ord}_p(a) = p-1$; equivalently, such that the list $1, a, a^2, a^3, \ldots, a^{p-2}$ contains each of the nonzero residues mod p exactly once. (Why are these equivalent?)*

The following problems sketch a proof of the above theorem (which you can cite in olympiads).

1. Suppose that $\operatorname{ord}_p(a) = x$ and $\operatorname{ord}_p(b) = y$, where x and y are relatively prime. Show that $\operatorname{ord}_p(ab) = xy$.

2. Show that if $d \mid p-1$, there are exactly d solutions to $x^d = 1$ in $\mathbb{Z}/p\mathbb{Z}^*$.

3. Suppose that q is a prime and q^{d_q} is the largest power of q dividing $n-1$. Show that there exists some $m \in \mathbb{Z}/p\mathbb{Z}^*$ such that $\operatorname{ord}_p(m) = q^{d_q}$.

4. Show that there exists a primitive root mod p.

The following criterion for primitive roots is useful:

Theorem 9. *An integer a is a primitive root modulo p if and only if for all primes q dividing $p-1$, $a^{(p-1)/q} \not\equiv 1 \pmod{p}$.*

You can define primitive roots likewise modulo any m, but usually they will not exist. For example, there are no primitive roots modulo pq if p and q are distinct odd primes.

Examples

5 (2009 Hungary-Israel). Let p be a prime. For which positive integers k is it the case that $\sum_{i=0}^{p-1} i^k \equiv 0 \pmod{p}$?

6. Determine whether there exist positive integers $n_1, n_2, \ldots, n_k$ all greater than 1 such that $n_1 \mid 2^{n_2} - 1$, $n_2 \mid 2^{n_3} - 1$, $\ldots$, $n_{k-1} \mid 2^{n_k} - 1$, $n_k \mid 2^{n_1} - 1$.

Problems

For some of these problems, like Problem 6 above, it is very helpful to start by arguing along the lines of "Let p be the smallest prime dividing (some number or set of numbers). Consider the order of (something) mod p..."

7 (Putnam 94/B6). For each non-negative integer i define $n_i = 101i + 100 \cdot 2^i$. If $0 \le a, b, c, d \le 99$ and $n_a + n_b \equiv n_c + n_d \pmod{101100}$, show that $\{a, b\} = \{c, d\}$.

8 (Putnam 97/B5). Define $a_1 = 2$, $a_n = 2^{a_{n-1}}$ for $n \ge 2$. Prove that $a_{n-1} \equiv a_n \mod n$.

9 (ELMO 2002?). Let n be an integer. Then every prime factor of $n^{2002} + n^{2001} + \ldots + n + 1$ is either equal to 2003 or is 1 mod 2003. (You may assume without proof that 2003 is prime. ☺)

10 (MOP 2000). Show that, for $n > 1$, if $3^n - 2^n$ is a prime power, then n is prime.

11 (IMO 99/4). Find all pairs of positive integers (n, p) such that

- p is a prime number

- $n \leq 2p$
- n^{p-1} divides $(p-1)^n + 1$.

12 (APMO 1997)**.** Find an integer n, $100 \leq n \leq 1997$ such that n divides $2^n + 2$.

13 (IMO 2003/6)**.** Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

14 (Bulgaria 96)**.** Find all pairs of primes (p, q) such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

15 (TST 03)**.** Find all triples p, q, r such that

$$p \mid q^r + 1, q \mid r^p + 1, r \mid p^q + 1.$$

16. (a) Find the smallest integer n with the following property; if p is an odd prime and a is a primitive root modulo p^n, then a is a primitve root modulo every power of p.

(b) Show that 2 is a primitive root modulo 3^k and 5^k for every positive integer k.

More useful facts:

Proposition 1. *If either p is an odd prime and $n \geq 1$, or $p = 2$ and $n \geq 2$, then, for integers a, b both relatively prime to p:*

$$a^p \equiv b^p \pmod{p^{n+1}} \iff a \equiv b \pmod{p^n}$$

Proposition 2. *Let p be a prime, $n \geq 2$, and k is a positive integer relatively prime to p. Assume additionally that $a \equiv b \pmod{p}$.*

$$a^k \equiv b^k \pmod{p^n} \iff a \equiv b \pmod{p^n}.$$

Additional Problems

17 (Ireland 1996)**.** Let p be a prime number and a, n positive integers. Prove that if $2^p + 3^p = a^n$, then $n = 1$.

18 (MOP 2000)**.** In how many zeroes does the number

$$4^{5^6} + 6^{5^4}$$

end?

19 (IMO Shortlist 1993)**.** A natural number n is said to have the property P, if, for all a, n^2 divides $a^n - 1$ whenever n divides $a^n - 1$.

(a) Show that every prime number n has property P.

(b) Show that there are infinitely many composite numbers n that possess property P.

20 (IMO Shortlist 2002)**.** Let $p_1, p_2, \ldots, p_n$ be distinct primes greater than 3. Show that $2^{p_1 p_2 \cdots p_n} + 1$ has at least 4^n divisors.

21. Show that there must either be infinitely many composite numbers of the form $2^{2^n} + 1$ or infinitely many composite numbers of the form $6^{2^n} + 1$. (Note: it is an open problem as to whether there exist infinitely composite numbers of the form $2^{2^n} + 1$; likewise it is an open problem as to whether there exist infinitely many composite numbers of the form $6^{2^n} + 1$; nevertheless we can show that one of the two sequences contains infinitely many composites.)

Extra problem

22 (MOP 2004)**.** Let m and n be positive integers such that 2^m divides the number $n(n+1)$. Prove that 2^{2m-2} divides the number $1^k + 2^k + ... + n^k$ for all positive odd integers k with $k > 1$.