Exponents and Primes

Alexander Remorov
alexanderrem@gmail.com

1 Some Fundamentals

Fundamental Theorem of Arithmetic: If n is a positive integer, it can be uniquely written as a product of primes: $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$.
Fermat's Little Theorem: If p is a prime, and a is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

- In problems dealing with finding/proving things about integers n, it is often useful to consider prime factorization of n, or specific prime factors of n.
- When you want to prove no positive integers n satisfying the conditions of the problem exist, assume one does exist, and look at the smallest such integer. Then find a smaller positive integer satisfying the conditions of the problem.
- Look at the smallest prime divisor or the largest prime divisor of n.
- It is sometimes useful to look at easy cases for n and then build up to the general case inductively. First prove the result when n is a prime, then when it is a power of a prime, then when it is a product of two powers of primes, etc. Or, induct on the number of prime divisors of n.

2 The Power of Factoring and Expanding

Here are two very well-known relations:
$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + ... + y^{n-1})$;
$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + ... + y^{n-1})$, if n is odd.
They turn out to be extremely useful when solving olympiad problems, because very often you encounter the expressions $a^n + b^n, x^n + 1, x^n - 1, a^n \equiv b^n \pmod{p}$.
Order of an Element
Let n be a positive integer and a a positive integer relatively prime to n. Let d be the smallest positive integer such that $a^d \equiv 1 \pmod{n}$. Then d is called the **order** of a modulo n, and is denoted by $\text{ord}_n a$.
Lemma 1: Let p be a prime, a a positive integer, $a \not\equiv 1 \pmod{p}$, and $d = \text{ord}_p a$. Then $1, a, a^2, ..., a^{d-1}$ are all different modulo n and $1 + a + ... + a^{d-1} \equiv 0 \pmod{p}$.

Proof. The first part follows by definition of d; the second part follows from $(a-1)(1+a+...+a^{d-1}) = a^d - 1 \equiv 0 \pmod{p}$ and the fact that p is a prime and $a \not\equiv 1 \pmod{p}$. □

Lemma 2: Let p be a prime, a a positive integer, and $d = \text{ord}_p a$. Then $d|(p-1)$.

Proof. Let $p-1 \equiv r \pmod{d}$ so $n = md + r$. Then $a^{p-1} = (a^d)^m a^r \equiv a^r \pmod{p}$. But $a^{p-1} \equiv 1 \pmod{p}$ so $a^r \equiv 1 \pmod{p}$. By definition of d and the fact that $0 \leq r < d$ is follows $r = 0$ and $d|(p-1)$. □

Lemma 3: Similarly, it follows if m is a positive integer, $d = \text{ord}_m a$, and $a^n \equiv 1 \pmod{p}$ then $d|n$.

Another simple relation, which is also very useful:
$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$

1. If $p|x$ then $(x+y)^n \equiv nxy^{n-1} + y^n \pmod{p^2}$.
2. More generally, if $p|x$, then $(x+y)^n \equiv \sum_{i=n-k+1}^{n} \binom{n}{i} x^{n-i} y^i \pmod{p^k}$.
3. In particular, if $a \equiv b \pmod{p}$ then $a = kp + b$ and so using 1, $a^n \equiv nkpb^{n-1} + b^n \pmod{p^2}$.

Lots of olympiad problems involve finding the highest power of a prime p dividing an integer n. We write $p^k||n$ if $p^k|n$ and $p^{k+1} \nmid n$. The following lemma was published by Santiago Cuellar and Jose Alejandro Samper in Mathematical Reflections 2007, Issue 3:

Lemma 4: Let p be an odd prime, a, b be two different integers not divisible by p, and n be a positive integer. Then if $a \equiv b \pmod{p}$, then if $p^k||(a-b), p^l||n$, then $p^{k+l}||(a^n - b^n)$.

Proof. It is enough to show that $p^l||\frac{a^n - b^n}{a-b}$. We will do this by induction on l.
Base Step: $l = 0$. Then $p \nmid n$ and:
$\frac{a^n - b^n}{a-b} = \sum_{i=0}^{n-1} a^{n-1-i} b^i \equiv \sum_{i=0}^{n-1} a^{n-1-i} a^i \pmod{p}$, since $a \equiv b \pmod{p}$, so
$\frac{a^n - b^n}{a-b} \equiv \sum_{i=0}^{n-1} a^{n-1} \pmod{p} \equiv na^{n-1} \pmod{p} \not\equiv 0 \pmod{p}$ since $p \nmid n$ and $p \nmid a$.
Induction Step: Assume $p^l||\frac{a^n - b^n}{a-b}$. We need to show $p||\frac{a^{pn} - b^{pn}}{a^n - b^n}$.
Now, $a^n \equiv b^n \pmod{p}$ then $b^n = kp + a^n$, so $b^{ni} \equiv ikpa^{n(i-1)} + a^{ni} \pmod{p^2}$ for $i = 1, 2, ..., n-1$.
Therefore:
$\frac{a^{pn} - b^{pn}}{a^n - b^n} = \sum_{i=0}^{p-1} a^{n(p-1-i)} b^{ni} \equiv \sum_{i=0}^{p-1} a^{n(p-1-i)} (ikpa^{n(i-1)} + a^{ni}) \pmod{p^2}$
$\equiv a^{n(p-2)} (\frac{kp^2(p-1)}{2} + pa^n) \pmod{p^2}$,
hence $p||\frac{a^{pn} - b^{pn}}{a^n - b^n}$. Then $p^{l+1}||\frac{a^{pn} - b^{pn}}{a-b}$ and the induction step is complete.

□

Lemma 5: Let a, b be two odd integers and n be a positive even integer. Then if $2^{k+1}||a^2 - b^2, 2^l||n$, then $2^{k+l}||(a^n - b^n)$.

Proof. It is enough to show that $2^{l-1}||\frac{a^n - b^n}{a^2 - b^2}$. We again use induction on l.
Base Step: $l = 1$. Then $n = 2m$ where m is odd, and:

$\frac{a^n-b^n}{a^2-b^2} = \sum_{i=0}^{n-1} a^{2(m-1-i)}b^{2i} \equiv \sum_{i=0}^{n-1} a^{2(m-1-i)}a^{2i} \pmod 2$, since $a \equiv b \pmod 2$, so

$\frac{a^n-b^n}{a-b} \equiv \sum_{i=0}^{n-1} a^{2(m-1)} \pmod 2 \equiv ma^{2(m-1)} \pmod 2 \not\equiv 0 \pmod 2$ since $2 \not| m$ and $2 \not| a$.

Induction Step: Assume $2^{l-1}||\frac{a^n-b^n}{a^2-b^2}$. We need to show $2||\frac{a^{2n}-b^{2n}}{a^n-b^n}$.

This follows from the fact that $\frac{a^{2n}-b^{2n}}{a^n-b^n} = a^n + b^n \equiv 2 \pmod 4$ since a^n, b^n are both congruent 1 modulo 4, since a, b are odd and $2|n$.

Hence $2||\frac{a^{2n}-b^{2n}}{a^n-b^n}$. Then $2^l||\frac{a^{2n}-b^{2n}}{a^2-b^2}$ and the induction step is complete.

□

Some important corollaries of the above results:

1. Lemmas 4 and 5 work for any integers a, b; so they will also work for expressions of the form $a^n + b^n$ if n is odd; just consider $-b$ instead of b.

2. In the expression $(a-b)(a^{n-1} + a^{n-2}b + ... + b^{n-1})$ the greatest common divisor of the two brackets is usually quite small. If an odd prime p divides the greatest common divisor of the two brackets, and $p \not| a$, then $p|n$ as well.

3. Let p be an odd prime. Then if $a \geq 2$, $a^p - 1$ has a prime divisor which does not divide $a - 1$. *Sketch of Proof:* Assume the contrary. Then $\gcd(a-1, a^{p-1} + a^{p-2} + ... + 1)|p$ so $a^{p-1} + a^{p-2} + ... + 1$ is a power of p. Using Lemma 4, $p^2||(a^p - 1)$ hence $a^{p-1} + a^{p-2} + ... + 1 = a - 1$, which gives a contradiction.

4. Let p be an odd prime. Then if $a \geq 2$, and $p \neq 3$ or $a > 2$ then $a^p + 1$ has at a prime divisor which does not divide $a + 1$.

Example: (Russia 1996) The positive integers a, b, p, n, k satisfy $a^n + b^n = p^k$. Show that if $n > 1$ is odd, and p is an odd prime, then n is a power of p.

Solution: First note that $p^k = (a+b)(a^{n-1} - a^{n-2}b + ... + b^{n-1})$ hence $a + b = p^j$ for some $j \geq 0$. Because $a + b \geq 2$ then $j \geq 1$.

Let l be such that $p^l||n$. Because $a \equiv -b \pmod p$, then using lemma 4, have $p^{l+j}||(a^n - (-b)^n) = p^k$. So $l + j = k$ and $l = k - j$.

Using lemma 4 again, have $p^k||(a^{p^{k-j}} + b^{p^{k-j}})$ and $a^{p^{k-j}} + b^{p^{k-j}}|a^n + b^n$ since n is odd and $p^{k-j}||n$. But $a^n + b^n = p^k$ so $p^k = a^{p^{k-j}} + b^{p^{k-j}} = a^n + b^n$ and $n = p^{k-j}$. The result follows.

3 Resources

1 *Santiago Cuellar, Jose Alejandro Samper, A Nice and Tricky Lemma, Mathematical Reflections*,
`http://reflections.awesomemath.org/2007_3/Lifting_the_exponent.pdf`

2 *Naoki Sato's Number Theory Package*,
`http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf`

3 *David Arthur's Handout from Winter Camp 2009*,
`http://www.stanford.edu/~darthur/wc09/numbertheory.pdf`

4 *Jacob Tsimerman's Handout from Winter Camp 2008*,
`http://web.mit.edu/yufeiz/www/wc08/nt.pdf`

5 *Yimin Ge's article on Vieta Jumping*,
`http://www.georgmohr.dk/tr/tr09taltvieta.pdf`

6 *Problems In Elementary Number Theory, Volumes 1 and 2*,
`http://projectpen.files.wordpress.com/2008/10/pen-vol-i-no-1.pdf`
`http://www.cpohoata.com/wp-content/uploads/2009/06/pen-vol-ii-no-1-090618.pdf`

4 Some Useful Results

The following problems are for warm-up, but the results in them are useful. It is good to know them.

1. If p is an odd prime, and $p \equiv 3 \pmod 4$, and $p|(x^2+y^2)$ show that $p|x$ and $p|y$.
   Corollary: If n is a positive integer, and p a prime dividing n^2+1, then $p \equiv 1 \pmod 4$.
   Note: If $n \equiv 3 \pmod 4$ then n has a prime divisor congruent to 3 modulo 4. It is often useful to look at prime divisors of n that are congruent to 3 modulo 4 or those congruent to 1 modulo 4.

2. Let a be an integer and m, n be positive integers. Prove: $\gcd(a^m-1, a^n-1) = |a^{\gcd(m,n)}-1|$.

3. If a is an integer not divisible by a prime p, and for some integer k, $a^k \equiv -1 \pmod p$ then if $d = \text{ord}_p a$, then $f = \frac{d}{2}$ is the smallest integer for which $a^{\frac{d}{2}} \equiv -1 \pmod p$.

4. **Euler's Theorem:** If n and a are positive integers, and $\gcd(a,n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod n$. (Here, $\phi(n)$ is the Euler function; if $n = p_1^{e_1}p_2^{e_2}...p_k^{e_k}$ then $\phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$.)
   You are allowed to use ONLY Fermat's Little Theorem and Lemma 4.
   Note: We can prove more: if $m = \text{lcm}(p_1-1, p_2-1, ..., p_k-1)$ then
   $a^{mp_1^{e_1-1}p_2^{e_2-1}...p_k^{e_k-1}} \equiv 1 \pmod n$.

5. Prove that the smallest positive integer d for which $2^d \equiv 1 \pmod{3^k}$ is $d = \phi(3^k)$.
   Note: A number a is called a **primitive root** modulo n if $\text{ord}_n a = \phi(n)$. This question shows that 2 is a primitive root modulo 3^n.
   Note: Using the note in question 3, and Lemma 4, show if a positive integer n has a primitive root then n is equal to $2, 4, p^k$, or $2p^k$ where p is an odd prime.

6. If x is a positive integer, and p, q are primes and $q|\dfrac{x^p-1}{x-1}$ then $q = p$ or $q \equiv 1 \pmod p$.

7. Let n be a positive integer. Show that all prime divisors of $2^{2^n}+1$ are congruent to 1 modulo 2^{n+1}.

5 Problems

The following problems are more difficult and are olympiad/easy IMO level.

1. Find the smallest positive integer n for which $2^{2010}|(17^n - 1)$.
2. (Putnam 2008) Let p be a prime and $P(x)$ be a polynomial with integer coefficients. If $P(0), P(1), ..., P(p^2-1)$ are distinct modulo p^2, prove that $P(0), P(1), ..., P(p^3-1)$ are distinct modulo p^3.
3. (IMO 1991.2) Let n be an integer greater than 6. If $a_1, a_2, ..., a_k$ are all positive integers, which are relatively prime to n and less than n, and $a_2 - a_1 = a_3 - a_2 = ... = a_k - a_{k-1} > 0$, show that n is prime or a power of 2.
4. (SL 1990 N5) Find the largest integer k such that 1991^k divides $1990^{1991^{1992}} + 1992^{1991^{1990}}$.
5. (IMO 1999.4) Find all pairs of positive integers (x, p) so that p is prime, $x \leq 2p$, and $x^{p-1}|(p-1)^x + 1$.
6. (IMO SL 2007.2) Let $b, n > 1$ be integers. For all $k > 1$, there exists an integer a_k so that $k|(b - a_k^n)$. Prove that $b = m^n$ for some integer m.
7. (China TST 2006) Find all pairs of integers (a, n) for which n divides $(a+1)^n - a^n$.
8. (IMO 1990.3) Find all positive integers n such that $\frac{2^n + 1}{n^2}$ is an integer.
9. (USA TST 2003) Find all triples of primes (p, q, r) such that $p|q^r + 1$, $q|r^p + 1$, $r|p^q + 1$.
10. (China TST 2005) Let a, m, n be positive integers such that $a > 1; m \neq n$. If $a^m - 1$ and $a^n - 1$ have the same prime divisors, prove that $a + 1$ is a power of 2.

Here are some harder problems. Many of these involve more than just the techniques discussed in this handout. If you can do the last few of them, you are quite well prepared if a problem on this subject appears on IMO.

1. (IMO 2000.5) Does there exist a positive integer n such that n has exactly 2000 different prime divisors and $2^n + 1$ is divisible by n?
2. (SL 2000 N4) Find all triples of positive integers (a, m, n) so that $a^m + 1|(a+1)^n$.
3. (USA TST 2008) Prove that there does not exist an integer n such that $n^7 + 7$ a perfect square.
4. (SL 2002 N3) Let $p_1, p_2, ..., p_n$ be distinct primes greater than 3. Prove that $2^{p_1 p_2 ... p_n} + 1$ has at least 4^n divisors.
5. (SL 2001 N4) Let $p > 5$ be prime. Show that there exists an integer a, $1 \leq a \leq p - 2$ so that $a^{p-1} - 1$ and $(a+1)^{p-1} - 1$ are both not divisible by p^2.
6. (SL 2005 N4) Find all positive integers n greater than 1, for which there exists a unique integer a, $0 < a < n!$ and $a^n + 1$ is divisible by $n!$.

7. (Russia 2001) Find all positive integers n such that for any coprime divisors a, b of n, the number $a + b - 1$ is also a divisor of n.

8. (IMO 2003.6) Let p be a prime number. Show that there exists a prime q such that for every integer n, $n^p - p$ is not divisible by q.

9. (SL 2005 N6) Let a, b be positive integers so that $(a^n + n)|(b^n + n)$ for all positive integers n. Prove that $a = b$.

10. (China TST 2005, Number Theory Problem 104) If n is a positive integer, $F_n = 2^{2^n} + 1$. Prove that for $n \geq 3$, there exists a prime factor of F_n which is larger than $2^{n+2}(n + 1)$.

11. (SL 2006 N5) Find all integers (x, y) satisfying the equation $\dfrac{x^7 - 1}{x - 1} = y^5 - 1$.

12. (Russia 2005) The positive integers x, y, z (with $x > 2, y > 1$) satisfy $x^y + 1 = z^2$. Let p be the number of prime divisors of x and q be the number of prime divisors of y. Show that $p \geq q + 2$.

(SL = IMO ShortList)