Orders and Exponents

Evan Chen

BNW-ORDERS

§1 Lecture Problems

We will follow *Orders Modulo a Prime* fairly closely, but you need not read it before-hand.
Tools:

- Orders / Fermat-Euler
- n^2+1 Theorem
- Lifting the Exponent

However, basically everything is really just based off two things: the fact that x^k+1 factors, and the fact that $a^{\varphi(n)} \equiv 1 \pmod n$.

§1.1 Orders

Definition. The *order* of $x \pmod n$ (where $\gcd(x,n) = 1$) is the smallest positive integer $e > 0$ such that $x^e \equiv 1 \pmod n$.

Theorem 1.1
If $x^m \equiv 1 \pmod n$ then the order of $x \pmod n$ divides m.

Proof. Division algorithm. □

Theorem 1.2 (Primitive roots)
For any prime p there exists a $g \pmod p$ with order exactly $p-1$.

Problem 1.3. How many primitive roots are there?

Theorem 1.4 (Fermat's Christmas theorem)
Let p be prime. Then there exists n such that $p \mid n^2+1$ if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Problem 1.5 (Online Math Open, Evan Chen)**.** Find the sum of all integers m with $1 \le m \le 300$ such that for any integer n with $n \ge 2$, if $2013m$ divides $n^n - 1$ then $2013m$ also divides $n-1$.

§1.2 Lifting

Problem 1.6. Compute
$$\nu_3(2^{3^n}+1).$$

Theorem 1.7 (Lifting the Exponent)
For $p > 2$, assume $0 \not\equiv x \equiv y \pmod p$. Then
$$\nu_p(x^n - y^n) = \underbrace{\nu_p(x-y)}_{>0} + \nu_p(n).$$

Problem 1.8. Show that there are no primitive roots modulo 2^n for $n \geq 3$.

Problem 1.9. What about other prime powers?

§2 Practice Problems

Problem 2.1 (British MO)**.** A number written in base 10 is a string of 3^{2013} digit 3's. No other digit appears. Find the highest power of 3 which divides this number.

Problem 2.2. Prove that 2 is a primitive root modulo 3^n for $n \geq 1$.

Problem 2.3 (PUMaC 2012)**.** Let $p_1 = 2012$ and $p_n = 2012^{p_{n-1}}$. Compute $\nu_{2011}(p_{2012} - p_{2011})$.

Problem 2.4 (IMO 2005/4)**.** Determine all positive integers relatively prime to all the terms of the infinite sequence
$$a_n = 2^n + 3^n + 6^n - 1,\ n \geq 1.$$

Problem 2.5 (HMMT November 2014)**.** Determine all positive integers $1 \leq m \leq 50$ for which there exists an integer n for which m divides $n^{n+1} + 1$.

Problem 2.6. For which primes p does there exist an integer x such that p divides $x^2 + 3$?