Stuff mod p^r: corrected version

Alison Miller

June 30, 2011

Please send typos, corrections, etc, to abmiller@math.princeton.edu.

1 Warm-up

1 (MOP 00)**.** How many zeroes are there at the end of

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

2 Basic Facts

For the purposes of this handout, p is an **odd** prime.[1]

$\mathbb{Z}/p^n\mathbb{Z}$ is the set of integers mod p. It has an addition and a multiplication law, furthermore, any element that is not a multiple of p has a multiplicative inverse. We can consider the subset $\mathbb{Z}/p^n\mathbb{Z}^*$ of invertible elements; these are exactly the elements not divisible by p. These form an abelian group, so we can use the language of group theory here, but we don't need to.

Definition 1. The order mod p^n of an element $a \in \mathbb{Z}/p^n\mathbb{Z}$ is the least d such that $a^d = 1 \mod p^n$.

Theorem 1. The multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$: The multiplicative group of $\mathbb{Z}/p^n\mathbb{Z}$ has order $\phi(p^n) = p^{n-1}(p-1)$ and is cyclic.

(You should prove this but you may assume that the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic.)

More useful terminology:

Definition 2. For an integer n define $v_p(n) = \max\{a : p^a \mid n\}$. This is often called the "p-adic valuation" of n.

Exercise 1. Show that $v_p(a+b) \geq \min(v_p(a), v_p(b))$.

Theorem 2.

$$(a+p^r b)^n = a^n + np^r a^{n-1}b \pmod{p^{2r}}.$$

mod p^n **analogue of Taylor Series:** If $P(x) \in \mathbb{Z}[x]$, then

$$P(a+p^r b) = P(a) + p^r bP'(a) + \frac{p^{2r}b^2P''(a)}{2!} + \frac{p^{2r}b^3P'''(a)}{3!} + \cdots.$$

In particular:

$$P(a+p^r b) = P(a) + p^r bP'(a) \pmod{p^{2r}}.$$

(Again, this sum is finite.)

[1] Unless stated otherwise.

Lemma 1 (Hensel's Lemma)**.** For a polynomial $P(x) \in \mathbb{Z}[x]$, if there exists $a \in \mathbb{Z}$ such that $P(a) \equiv 0 \pmod{p}$, and $P'(a) \not\equiv 0 \pmod{p}$, then, for any positive integer k, there exists $b \in \mathbb{Z}$ with $b \equiv a \pmod{p}$ and $P(b) \equiv 0 \pmod{p^n}$.

The sort of inductive construction used in Hensel's Lemma can be useful in other contexts as well.

Lemma 2 (The Lemma Which is Not Hensel's Lemma, a.k.a. Lifting the Exponent)**.** Let p be an odd prime and n a positive integer.

If $v_p(a) = v_p(b) = 0$ and $v_p(a - b) > 0$, then $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$.

Corollary 1. Let p be an odd prime and n an odd positive integer.

If $v_p(a) = v_p(b) = 0$ and $v_p(a + b) > 0$, then $v_p(a^n + b^n) = v_p(a + b) + v_p(n)$.

(The prime $p = 2$ is finicky, so we won't talk about it here. But analogous statements do exist; can you find them?)

The formula for $v_p(n!)$ is useful; it can also be used to find the p-adic valuation of binomial coefficients.

Theorem 3 (Wolstenholme's theorem:)**.** This is a name given to a number of related facts. Here, let p be a prime greater than or equal to 5. Then the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2 and the numerator of

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$$

is divisible by p.

$$\binom{2p}{p} \equiv 2 \pmod{p^3},$$

and more generally

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}.$$

3 Problems

Not all the problems below involve prime powers in their statements, so you may need to focus on certain primes or apply Chinese Remainder theorem to solve them.

2. (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.

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

4. Find all pairs (m, n) of positive integers, with $m, n \geq 2$, such that $a^n - 1$ is divisible by m for each $a \in \{1, 2, \dots, n\}$.

5 (USA TST)**.** Let p be a prime number greater than 5. For any integer x, define

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2}$$

Prove that for all positive integers x and y the numerator of $f_p(x) - f_p(y)$, when written in lowest terms, is divisible by p^3.

6. Show that the equation $x^n + y^n = (x+y)^m$ has a unique solution satisfying $x > y$, $m > 1$, $n > 1$.

7 (China TST 2004, MOP 2004)**.** Let u be a fixed positive integer. Prove that the equation $n! = u^\alpha - u^\beta$ has a finite number of solutions (n, α, β).

8 (IMO Shortlist 2007)**.** For every integer $k \geq 2$, prove that 2^{3k} divides the number

$$\binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

but 2^{3k+1} does not.

9 (MOP '08)**.** Let a, b, c, d, m be positive integers such that $\gcd(m, c) = 1$. Prove that there exists a polynomial f of degree at most d such that $f(n) \equiv c^{an+b} \pmod{m}$ for all n if and only if m divides $(c^a - 1)^{d+1}$.

4 Factorials, Binomial coefficients, etc

Let p be an odd prime.

We know that $n!$ is divisible by a high power of p. In fact... $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots$. So looking at $n!$ modulo powers of p is boring, because there are all those p's in them. Let's take them out!

Definition 3. Let

$$(n!)_p = \prod_{\substack{1 \leq i < n \\ p \nmid i}} i.$$

This is however a suboptimal definition because it turns out that the value of $(n!)_p$ mod p^n depends not only on the value of n mod p but also on the parity of p (look at $(1!)_p$ versus $(p+1)!_p)$.

The mathematicians who have thought about this sort of thing have generally worked in terms of generalizing the Γ function $\Gamma(n) = (n-1)!$, so we will use their terminology.

The following definition fixes both those problems.

Definition 4 (Morita's p-adic gamma function)**.** Let

$$\Gamma_p(n) = (-1)^n \Gamma_p(n-1).$$

.

Theorem 4. If $a \equiv b \pmod{p^n}$, then $\Gamma_p(a) \equiv \Gamma_p(b) \pmod{p^n}$.

(Note: this implies that Γ_p can be extended to a continuous function on the p-adics.)

10. Suppose p is 1 mod 4. Show that if $2a \equiv 1 \pmod{p^n}$ then $\Gamma_p(a)^2 \equiv -1 \pmod{p^n}$.

Because of this we can say that $\Gamma_p(1/2)$ is a p-adic square root of -1.

5 Bonus: TST 2010 and Beyond

[WARNING: this section was written late at night and may contain typos/mistakes.]

This problem should be familiar:

11 (TST 2010)**.** Determine whether or not there exists a positive integer k such that $p = 6k + 1$ is a prime and

$$\binom{3k}{k} \equiv 1 \pmod{p}.$$

While (trying to) solve it, one might make the observation that

$$\binom{3k}{k} \equiv -\sum_{i \mod p} i^{4k}(1+i)^{3k} \pmod{p}$$

(The sum above is the sum as i runs through all of the p distinct residues mod p.)

and also

$$0 \equiv \sum_{i \mod p} i^{2k}(1+i)^{3k} \pmod{p}.$$

Let's generalize if $p = nk + 1$, then for positive integers a, b with $0 < a, b < n$:

12. Show

$$\sum_{i \mod p} i^{ak}(1+i)^{bk} \pmod{p} = \begin{cases} 0 & \text{if} a + b < n \\ \binom{bk}{(a+b-n)k} \pmod{p} & \text{if} a + b \geq n. \end{cases}$$

(Side question; what happens if you switch a and b?)

Why is this in this handout? Well, it has a mod p^n generalization, as follows:

13. Let $k_n = (p^n - 1)/a$, so $k_1 = k$. Show

$$\sum_{i \mod p} i^{akp^{n-1}}(1+i)^{bkp^{n-1}} \pmod{p} = \binom{bk_n}{(a+b-n)k_n}_p \pmod{p^n} \text{ if} a + b \geq n.$$

Where $\binom{m}{n}_p$ should be something defined analogously to $(n!)_p$. (Side note; if you know what the beta function is, this sort of looks like the integral definition of the beta function.)

(Reality checks you ought to make: Why does it even make sense to consider the left hand side mod p^n, given that i is only defined mod p? Also, you should check that the mod p^n results you are getting for different n are consistent with each other. If you think there is a mistake in this, send me an e-mail at abmiller@math.princeton.edu. Also I think the $a + b \geq n$ condition may be unnecessary.)

This should follow from the work of some subset of {Gross-Koblitz, Katz, Dwork} using very advanced methods. I don't know an olympiad-level proof but am curious if one exists (even one that only works for special cases).

Appendix to last time: the correct version of Siegel's Theorem

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree at least 3 with distinct roots. Then the equation $y^2 = f(x)$ has only finitely many solutions in $\mathbb{Z}$. (This is actually a special case of the full Siegel's theorem for integer points on curves, but it's a form which is easy to cite and apply accurately.)

However, it certainly can have infinitely many solutions in $\mathbb{Q}$ if f has degree 3 or 4. (This is true by the theory of elliptic curves; doing an explicit example is messy but I'd like to see one if anyone has one.)