Binomial Coefficients and p-adic Continuity

Masha Vasenko
UCD mathsoc talk

26/09/13

continuous function

$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad$ s.t.

$|f(x) - f(y)| < \varepsilon$

when $|x - y| < \delta$

(I) $f : \mathbb{N} \to \mathbb{N}$

$f(1), f(2), f(3), \ldots$

sequence of natural numbers

fix a prime number p

We call f a "good" function

if $\forall M \quad \exists N \quad$ s.t.

$p^M \mid (f(x) - f(y))$

when $p^N \mid (x - y)$.

Example 1 (polynomial functions are "good")

$$f(x) = \sum_{i=0}^{k} a_i x^i \qquad a_i \in \mathbb{N} \ (\text{or } a_i \in \mathbb{Z})$$

$$f(x) - f(y) = \sum_{i=1}^{k} a_i (x^i - y^i)$$

$$= (x-y)\left(\sum_{i=1}^{k} a_i (x^{i-1} + x^{i-2}y + \ldots + y^{i-1})\right)$$

$$p^N \mid (x-y) \implies p^N \mid (f(x) - f(y))$$

(Counter) Example 2

$f(x) = a^x \qquad a \in \mathbb{N}$

power function isn't always good

$$f(x) - f(y) = a^y \left(a^{x-y} - 1 \right)$$

(let $x > y$)

we could fix y
& take $x = y + p^N$

We want

$$p^* \mid a^{p^N} - 1$$

Fermat's Little Theorem: $a^p \equiv a \mod p$

$f(x) = a^x$ isn't "good"
when $a \not\equiv 1 \mod p$.

Suppose now that $a \equiv 1 \mod p$:

$$a = 1 + pb$$

$$a^{p^N} = (1 + pb)^{p^N}$$

$$= \sum_{k=0}^{p^N} \binom{p^N}{k} p^k b^k$$

$$= 1 + \binom{p^N}{1} pb + \binom{p^N}{2} p^2 b^2 + \dots$$

let us show that these binomial coefficients are divisible by some high powers of p

Lemma $\quad ord_p\left(\binom{p^N}{k} p^k\right) \geq N+1$

when $\quad 1 \leq k < p^N$.

From this lemma, it follows that

$$a^{p^N} \equiv 1 \mod p^{N+1}$$

when $a \equiv 1 \mod p$. And therefore

$f(x) = a^x$ is "good"

if and only if $a \equiv 1 \mod p$.

Proof of Lemma $\quad \binom{n}{k} = \frac{n!}{k!(n-k)!}$

$$ord_p \binom{n}{k} = ord_p(n!) - ord_p(k!) - ord_p((n-k)!)$$

$\rightsquigarrow$ would be nice to have a formula for $ord_p(n!)$

$n! = 1 \cdot 2 \cdot \ldots \cdot n$

$\lfloor \frac{n}{p} \rfloor$ numbers divisible by p

$\lfloor \frac{n}{p^2} \rfloor$ ... p^2

$\lfloor \frac{n}{p^3} \rfloor$ ... p^3

...

$$ord_p(n!) = \lfloor \tfrac{n}{p} \rfloor + \lfloor \tfrac{n}{p^2} \rfloor + \lfloor \tfrac{n}{p^3} \rfloor + \ldots$$

Let's write n to the base p:

$$n = a_0 + a_1 p + a_2 p^2 + \ldots + a_s p^s$$

$$n = \overline{a_s a_{s-1} \dots a_0}^{(p)}$$

Then $\left\lfloor \frac{n}{p} \right\rfloor = \overline{a_s a_{s-1} \dots a_1}^{(p)}$

$$= a_s p^{s-1} + \dots + a_2 p + a_1$$

$$\left\lfloor \frac{n}{p^2} \right\rfloor = a_s p^{s-2} + \dots + a_2$$

$$\dots$$

$$\Rightarrow \operatorname{ord}_p(n!) = a_s (p^{s-1} + p^{s-2} + \dots + 1)$$
$$+ a_{s-1} (p^{s-2} + p^{s-3} + \dots + 1)$$
$$+ \dots$$
$$+ a_1$$
$$= a_s \frac{p^s - 1}{p-1}$$
$$+ a_{s-1} \frac{p^{s-1} - 1}{p-1}$$
$$+ \dots$$
$$+ a_1 \frac{p-1}{p-1}$$

$$= \frac{(a_s p^s + a_{s-1} p^{s-1} + \dots + a_1 p + a_0) - (a_s + a_{s-1} + \dots + a_0)}{p-1}$$

$$= \boxed{\frac{n - S_n}{p-1} = \operatorname{ord}_p(n!)}$$

where S_n = the sum of p-adic digits of n

Back to the Lemma:

$$\mathrm{ord}_p\binom{n}{k} = \frac{S_k + S_{n-k} - S_n}{p-1}$$

Let now $n = p^N$, $1 \le k < p^N$

$$k = \overline{\ldots a_1 a_0}^{(p)}$$

$$p^N - k = \overline{\ldots b_1 b_0}^{(p)}$$

$$p^N = \overline{100\ldots00}^{(p)}$$

It follows that there are

$$\ell = \mathrm{ord}_p(k) = \mathrm{ord}_p(p^N - k)$$

zeros at the end, i.e.

$$a_0 = \ldots = a_{\ell-1} = b_0 = \ldots = b_{\ell-1} = 0,$$

and then

$$a_\ell + b_\ell = p$$
$$a_{\ell+1} + b_{\ell+1} = p-1$$
$$a_{\ell+2} + b_{\ell+2} = p-1$$
$$\ldots$$
$$a_{N-1} + b_{N-1} = p-1.$$

Therefore

$$\mathrm{ord}_p\binom{p^N}{k} = \frac{\overbrace{S_k + S_{p^N-k}}^{1+(p-1)(N-\ell)} - 1}{p-1}$$

$$= N - \ell = N - \mathrm{ord}_p(k).$$

And

$$\mathrm{ord}_p\left(\binom{p^N}{k} p^k\right) = N - \mathrm{ord}_p(k) + k \ge N+1$$

since $k \ge \mathrm{ord}_p(k) + 1$. ☒

Here is a more simple argument for the Lemma:

$$\binom{p^N}{k} = \frac{p^N (p^N-1)\cdots(p^N-k+1)}{k\cdot(k-1)\cdot\ldots}$$

$$= \frac{p^N}{p^N-k}\underbrace{\binom{p^N-1}{k}}_{\text{integer number}}$$

$$\Rightarrow \quad ord_p\binom{p^N}{k} \geq N - ord_p(p^N-k)$$

$$= N - ord_p(k)$$

But in the above proof we have even seen that this inequality is an equality, and $p \nmid \binom{p^N-1}{k}$.

We gave such a long proof because the formulas

$$ord_p(n!) = \frac{n - S_n}{p-1}$$

and $$ord_p\binom{n}{k} = \frac{S_k + S_{n-k} - S_n}{p-1}$$

will be interesting to us in the future. (These formulas were known to Gauss.)

(Counter) example 3

$$f(x) = x!$$

is not good:

$$f(x) - f(y) = y!\left(\prod_{y<j'\le x} j - 1\right)$$
$$x > y$$

would be "good" if

$$p^* \mid \left(\prod_{y<j\le y+p^N} j - 1\right)$$

but this product is itself divisible by high powers of p when N is large, so it can't be the case with (the product -1).

Let's try to repair the situation:

$$f(x) = \prod_{\substack{1\le j'\le x \\ p\nmid j}} j \quad \left(= \frac{x!}{\left\lfloor \frac{x}{p} \right\rfloor ! \cdot p^{\left\lfloor \frac{x}{p} \right\rfloor}}\right)$$

$$\downarrow$$

$$p^* \mid \left(\prod_{\substack{y<j\le y+p^N \\ p\nmid j}} j - 1\right)$$

Trouble: Wilson's congruence

$$(p-1)! \equiv -1 \mod p$$

Therefore $\prod_{\substack{y<j\le y+p^N \\ p\nmid j}} j \equiv ((p-1)!)^{p^N} \mod p$

assume $p \neq 2$ from now on

$$\equiv (-1)^{p^N} \mod p$$

$$\equiv -1 \mod p,$$

so the difference

$$\prod_{\substack{y<j\le y+p^N \\ p\nmid j}} j - 1$$

can't be divisible by a high power of p.

We can repair this problem as follows: define

$$f : \mathbb{N} \to \mathbb{Z}$$

$$f(x) = (-1)^x \prod_{\substack{1\le j\le x \\ p\nmid j}} j$$

"p-adic factorial"

<u>Theorem</u> p-adic factorial is a "good" function. Namely,

if $p^N \mid (x-y)$
then
$$p^N \mid (f(x) - f(y)).$$

<u>Proof</u> Wilson's congruence admits the following generalisation:

$$\prod_{\substack{1 \le j < p^N \\ p \nmid j}} j \equiv -1 \mod p^N.$$

(The proof is analogous. Exercise.)

Let now $x = y + mp^N$:

$$f(y + mp^N) - f(y)$$

$$= f(y) \Big(\underbrace{\underbrace{(-1)^{mp^N}}_{= (-1)^m} \underbrace{\prod_{\substack{y < j \le y + mp^N \\ p \nmid j}} j}_{\equiv (-1)^m} - 1}_{\equiv 0 \mod p^N} \Big)$$

$\mod p^N$

$\boxtimes$

Here are many more examples of "good" functions similar to the factorial.

Generalised binomial coefficients:

$$\theta \in \mathbb{Q} \setminus \{0, -1, -2, -3, \dots\}$$

$$A_\theta(n) = \frac{\theta(\theta+1)\dots(\theta+n-1)}{n!}$$

$$\left(= \binom{\theta+n-1}{n} \text{ when } \theta \in \mathbb{N} \right)$$

Theorem (B. Dwork, "p-adic cycles", 1969)

Suppose p doesn't divide the denominator of θ. We define θ' as the (unique) rational number whose denominator is not divisible by p and such that

$$p\theta' - \theta \in \{0, 1, \dots, p-1\}.$$

Then

$$f(n) = \frac{A_\theta(n)}{A_{\theta'}\left(\left[\frac{n}{p}\right]\right)}$$

is a "good" function. Namely,

$$p^N \mid \left(f(n+mp^N) - f(n) \right)$$

(in a sense that it divides the numerator of this rational number).

Example 4 $\theta = \frac{1}{2}$ $\quad p \neq 2$

$\theta' = \frac{1}{2}$ since $\frac{p-1}{2} \in \{0, 1, \dots, p-1\}$.

$$A_{\frac{1}{2}}(n) = \frac{\frac{1}{2}\left(\frac{1}{2}+1\right)\dots\left(\frac{1}{2}+n-1\right)}{n!}$$

$$= \frac{1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)}{2^n\, n!}$$

$$= \frac{(2n)!}{4^n (n!)^2} = \frac{1}{4^n}\binom{2n}{n}$$

So, according to the Theorem

$$f(n) = 4^{\lfloor \frac{n}{p} \rfloor - n} \frac{\binom{2n}{n}}{\binom{2\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{n}{p} \rfloor}} \quad \text{is "good".}$$

Let us show that 4^* isn't essential here – one can remove this factor. Consider

$$g(n) = 4^{n - \lfloor \frac{n}{p} \rfloor} f(n) = \frac{\binom{2n}{n}}{\binom{2\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{n}{p} \rfloor}}.$$

Then

$$g(n+mp^N) - g(n)$$

$$= \underbrace{4^{m(p^N - p^{N-1})}}_{= \left(4^{(p-1)}\right)^{p^{N-1} \cdot m}} 4^{n - \lfloor \frac{n}{p} \rfloor} f(n+mp^N) - 4^{n - \lfloor \frac{n}{p} \rfloor} f(n)$$

$$4^{(p-1)} \equiv 1 \mod p \Rightarrow 4^{(p-1)p^{N-1}} \equiv 1 \mod p^N$$

(see example 2 before)

So, $p^N \mid (g(n+mp^N) - g(n))$.

where $g(n) = \frac{c_n}{c_{\lfloor \frac{n}{p} \rfloor}}$, $c_n = \binom{2n}{n} = \frac{(2n)!}{(n!)^2}$

Table of values of $g(n)$:

n	0	1	2	3	4	5	6	7
$p=3$	1	2	6	10	35	126	154	572
$p=5$	1	2	6	20	70	126	462	1716

n	8	9	10	11	
$p=3$	2145	2431	$\frac{46189}{5}$	$\frac{176358}{5}$	...
$p=5$	6435	24310	$\frac{92378}{3}$	117572	

$p=3$ $\quad g(10) - g(7) = \frac{46189}{5} - 572$

$= 3 \cdot \frac{14473}{5}$

$g(7) - g(4) = 572 - 35 = 3 \cdot 179$

$g(4) - g(1) = 35 - 2 = 3 \cdot 11$

$g(10) - g(1) = \frac{46189}{5} - 2 = 9 \cdot \frac{5131}{5}$

Question with $c_n = \frac{(3n)!}{(n!)^3}, \frac{(4n)!}{(n!)^4}, \frac{(5n)!}{(n!)^5}, \ldots$?

Part II : p-adic numbers

$\mathbb{Q}$ the field of rational numbers

A norm on a field F is a map $\|\cdot\| : F \to \mathbb{R}_{\geq 0}$ such that

1) $\|x\| = 0 \iff x = 0$
2) $\|x \cdot y\| = \|x\| \cdot \|y\|$
3) $\|x + y\| \leq \|x\| + \|y\|$

$d(x,y) := \|x - y\|$ turns F into a metric space

For example, the absolute value $|x|$ is a norm on $\mathbb{Q}$, and the closure of $\mathbb{Q}$ with respect to $d(x,y) = |x-y|$ is $\mathbb{R}$, the "real line".

Now fix a prime p and define another metric on $\mathbb{Q}$:

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p(x)}} & x \neq 0 \\ 0 & x = 0 \end{cases}.$$

Exercise: check properties 1) - 3).

The closure of $\mathbb{Q}$ w.r.t. $d(x,y) = |x-y|_p$ is called $\mathbb{Q}_p$, the field of p-adic numbers.

(See Chapter 1 in N. Koblitz, "p-adic numbers, p-adic analysis and zeta-functions")

$$\mathbb{Z}_p = \{ x \in \mathbb{Q}_p : |x|_p \leq 1 \}$$
$$\Leftrightarrow \operatorname{ord}_p(x) \geq 0$$

is the ring of p-adic integers. p-adic integers can be described as follows:

$$\{ a_n ; n \geq 1 \} \qquad 0 \leq a_n < p^n - 1$$
$$a_n \equiv a_{n-1} \bmod p^{n-1}$$

We have $\mathbb{N} \subset \mathbb{Z}_p$, natural numbers being correspondent to the sequences, whose terms stay the same after some point.

E.g. -1 corresponds to the sequence

$$\underset{a_1}{p-1}, \underset{a_2}{p^2-1}, \underset{a_3}{p^3-1}, \ldots$$

$$a_n = p^n - 1 \equiv -1 \bmod p^n$$

An interesting observation is that $\mathbb{N}$ is dense in $\mathbb{Z}_p$. So, every "good" function from the first part of

the talk defines a unique continuous function on $\mathbb{Z}_p$.

Now we can ask about its values at p-adic integers other than $\mathbb{N}$, for example ordinary negative integers:

$$f(-1) = \lim_{N \to \infty} f(p^N - 1)$$

must exist.

Can one evaluate this limit in our examples?
