Three perspectives on p-adic numbers: analytic, algebraic, topological

Nicolas Diaz-Wahl

Abstract

I outline the 3 main approaches to the construction of the p-adic numbers. The analytic approach constructs $\mathbb{Q}_p$ by taking the completion of $\mathbb{Q}$ with respect to the nonarchimedean absolute values, and classfies the nonarchimedean absolute values on $\mathbb{Q}$ as the p-adic ones. The algebraic approach defines completions with respect to topologies given by filtrations using inverse limits. Finally, Weil's topological approach starts with a nonarchimedean local field in characteristic zero, and shows that such fields are precisely the p-adic fields. These three approaches give various insights into the p-adics. Local compactness is emphasized.

1 Introduction: Why p-adic numbers?

I'll start by motivating p-adic numbers. To do so, I'll take a perspective that's not any of those; instead think (algebro) geometrically.

Take $R = k[T_1, \ldots, T_n]$. What does it mean to evaluate a polynomial? Take $f(\underline{T}) \in R$ and $\underline{t} = t_1, \ldots, t_n \in k$. One can evaluate $f(t)$ by using the field operations, but also can be done by reduction mod $(T_1 - t_1, \ldots, T_n - t_n)$. Indeed, long division sort of works, so you have

$$f(T) = g_1(T_1 - t_1) + \cdots + g_n(T)(T_n - t_n) + r(T)$$

with $\deg r(t_1) < 1$ with respect to t_1 for instance. Since $r(T) = f(T) - g_1(T)(T_1 - t_1) - \cdots - g_n(T)(T_n - t_n)$, we have $r(T) \in (T_1 - t_1, \ldots, T_n - t_n)$, so do long division again with respect to t_2, etc. until $f(\underline{T}) = g(\underline{T})(T_1 - t_1, \ldots, T_n - t_n) + c$. Clearly $f(\underline{t}) = c$.

Number theorists are interested in $\mathbb{Z}$ (and $\mathbb{Q}$ and stuff). There are a lot of formal similarities between $\mathbb{Z}$, $\mathbb{Q}$, and their extensions, and $k[T]$, $k(T)$, and their *separable* extensions. For instance $\mathbb{Z}$ and $k[T]$ are both PIDs. Taking $k = \mathbb{F}_q$, they both have finite residue fields. Let's see if we can "evaluate function" on $\mathbb{Z}$. Taking $f \in \mathbb{Z}$, then by analogy with the above, evaluating f at p should be the map $f \mapsto f \bmod p$. What a weird operation!

Let's talk about series expansions. In $k[T]$ (one variable this time), fix a point $t \in k$, and let $f(T) = g_1(T)(T-t) + r_1(T)$. Then let $g_1(T) = g_2(T)(T-t) + r_2(T)$, so $f(T) = (g_2(T)(T-t) + r_2(T))(T-t) + r_1(T) = g_2(T)(T-t)^2 + r_2(T)(T-t) + r_1(T)$. Note that $\deg g_n(T)$ and $\deg r_n(T)$ are strictly decreasing, so

$$f(T) = a_0(T-t)^n + a_1(T-t)^{n-1} + \cdots + a_0$$

with the $a_i \in k[T]/(T-t) \simeq k$. In exactly the same way, we can take a "base p expansion" of an integer f:

$$f = f_0 p^n + f_1 p^{n-1} + \cdots + f_n$$

with the f_i “ $\in$ ” $\mathbb{Z}/p\mathbb{Z}$ “ $=$ ” $\{0, 1, \dots, p-1\}$. Now the f_i are actually integers, but they behave as if the “came from” $\mathbb{Z}/p\mathbb{Z}$.

We can form two kinds of localization: $k[T, (T-t)^{-1}]$ and $k[T]_{(T-t)}$. In the former, functions have a singularity at t, and in the latter, they can have a singularity anywhere *except* at t. In $\mathbb{Z}$, the analogues are

$$\mathbb{Z}[1/p], \quad \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \; : \; p \nmid b \right\}.$$

The p-adic numbers “complete” the latter ring by allowing power series in p converging “in a neighborhood of p”. We have familiar expressions like

$$\frac{1}{1-p} = 1 + p + p^2 + \cdots$$

analogous to

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots, \quad |x| < 1.$$

2 Analytic view

To give a definition of the p-adic numbers, let's introduce a metric on $\mathbb{Z}$.

Definition 1. Let R be a ring. A *valuation* on R is a function

$$v : R \to \mathbb{R} \cup \{\infty\}$$

such that

(a) $v(xy) = v(x) + v(y)$

(b) $v(x + y) \geq \min\{v(x), v(y)\}$.

(c) $v(R - \{0\}) \subset \mathbb{R}$.

An *absolute value* is a function $|\cdot| : R \to \mathbb{R}$ such that

1. $|xy| = |x||y|$.
2. $|x + y| \leq |x| + |y|$.
3. $|x| = 0$ iff $x = 0$.

Two absolute values $|\cdot|_1$, $|\cdot|_2$ are *equivalent* if $|x|_1 = |x|_2^s$ for some $s > 0$. A *place* is an equivalence class of absolute values. Valuations and absolute values are related by

$$|x| = c^{-v(x)}, \quad v(x) = -\log_c |x|$$

for some $c > 0$.

$|\cdot|$ is *nonarchimedean*, hence $|nx|$ is bounded for $n \in \mathbb{Z}$.

Lemma 1. *We have that $|\cdot|$ is nonarchimedean if and only if $|x + y| \leq \max\{|x|, |y|\}$.*

Proof. Clearly the "only if" holds. Conversely, suppose WLOG $|x| \geq |y|$, and let $n \geq 0$. Then

$$|x+y|^n = \sum_{k=0}^{n} \left| \binom{n}{k} \right| |x|^k |y|^{n-k} \leq \sum_{k=0}^{n} N|x|^n = (n+1)N|x|^n.$$

Take nth roots and the limit as $n \to \infty$. □

Theorem 2 (Ostrowski)**.** *Let $|\cdot|$ be an absolute value on $\mathbb{Z}$. Either*

(a) $|\cdot|_0$ *the trivial absolute value.*

(b) *The usual absolute value.*

(c) *A p-adic absolute value: $|p| < 1$ for p prime, and $|\ell| = 1$ for all primes $\ell \neq p$.*

Proof. Assume $|\cdot|$ is nontrivial. There are two possibilities: (1) $|\cdot|$ is *archimedean*, i.e. for all $M > 0$ and $x \in \mathbb{Z}$, there is some $n \in \mathbb{Z}$ such that $|nx| > M$. It is standard real analysis to show that any such absolute value is equivalent to the usual one. This is the hardest part of the proof.

(2) Suppose $|\cdot|$ is nonarchimedean, hence $|nx|$ is bounded for $n \in \mathbb{Z}$. Then $|x+1|$ Since it is nontrivial, there is some integer n_0 such that $|n_0| < 1$. Since $|xy| = |x||y|$, there is some prime p such that $|p| < 1$. Let

$$\mathfrak{a} = \{n \in \mathbb{Z} \,:\, |n| < 1\}.$$

This is obviously an nontrivial ideal ($|1| = 1$ and the Lemma). We claim that $\mathfrak{a} = p\mathbb{Z}$. Firstly, we claim that $|n| \leq 1$ for all $n \in \mathbb{Z}$. Let ℓ be the smallest prime for which $|\ell| \neq 1$. Indeed, $|x| \leq \max\{|x-1|, |1|\} \leq \max\{|x-1|, |1|\}$, so $|x| \leq 1$ for all $0 \leq x < \ell$. Hence $|\ell| = |\ell - 1 + 1| \leq \max\{|\ell - 1|, |1|\} \leq 1$, so $\ell = p$, otherwise $\mathfrak{a} = \mathbb{Z}$, contradicting $1 \notin \mathfrak{a}$. □

We normalize the p-adic absolute value so that $|p|_p = 1/p$. Hence $|\mathbb{Z}|_p = p^{\mathbb{Z}_{\geq 0}} \cup \{0\}$, and you can clearly extend $|\cdot|_p$ to $\mathbb{Q}$ so $|\mathbb{Q}|_p = p^{\mathbb{Z}} \cup \{0\}$.

Proposition 3. *Let F be a field with an absolute value $|\cdot|$. Then $R := \{x \in R \,:\, |x| \leq 1\}$ is a local ring with unique maximal ideal $\mathfrak{m} = \{x \in R \,:\, |x| < 1\}$.*

Proof. Trivial. □

Definition 4. Let $\mathbb{Q}$ have the p-adic absolute value. It's valuation ring is $\mathbb{Z}_{(p)}$ with principal maximal ideal $p\mathbb{Z}_{(p)}$. We have $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$.

Taking the completion of $\mathbb{Q}$ with respect to this absolute value, we obtain the p-adic numbers $\mathbb{Q}_p$.

Proposition 5. *The ring $\mathbb{Q}_p$ is locally compact with compact open subring $\mathbb{Z}_p$. The ideal $p\mathbb{Z}_p$ in $\mathbb{Z}_p$ is maximal, open and closed, and induces the topology on $\mathbb{Q}_p$ via the filtration $\{p^i\mathbb{Z}_p\}_{i \in \mathbb{Z}}$. In particular, $\mathbb{Q}_p$ is totally disconnected.*

Proof. Everything follows once we show that $\mathbb{Z}_p$ is compact, which we show later using algebra. We leave it as an easy exercise to show that $\mathbb{Z}_p$ is open and closed. Hint: show that $|x+y| = \max\{|x|, |y|\}$ if $|x| \neq |y|$. □

Proposition 6. *Let $R = \{0, 1, \ldots, p-1\}$ be the set of standard representatives mod p. Then a p-adic integer can be written as*

$$\sum_{n \geq 0} a_n p^n, \ \ a_n \in R,$$

and a p-adic number can be written as

$$\sum_{n \geq m} a_n p^n, \ \ a_n \in R, \ m \in \mathbb{Z}.$$

Proof. An integer is of the form $f_n = a_0 + a_1 p + \cdots + a_n p^n$. If f is a p-adic integer, then f is a p-adically Cauchy sequence of integers f_n. Taking a subsequence if necessary, we may assume that $p^{\min\{n,m\}} | (f_n - f_m)$ for all $m, n \geq 0$. Hence $p^n | (f_n - f_{n+1})$ for all $n \geq 0$; write $f_{n+1} - f_n = c_n p^n$, so $f_{n+1} = f_n + c_n p^n$. By induction, we have that $f_n = a_0 + a_1 p + \cdots + a_n p^n$ for some a_i (independent of $n \geq 0$), so f is identified with

$$\lim_{n \to \infty} f_n = \sum_{n \geq 0} a_n p^n.$$

Since $f_{n+1} \equiv f_n \bmod p^n$, we have $f_{n+1} - f_n = p^n c + a_{n+1}$ with $a_{n+1} \in \{0, \ldots, p-1\}$, so by induction, we win. □

Corollary 7. *$\mathbb{Z}_p / p^n \mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. This follows at once from the p-adic expansion. □

Exercise 1. Extend the whole discussion to number fields and their rings of integers. Can you do this for function fields? What about arbitrary Dedekind domains? Read Neukirch *Algebraic Number Theory* if you haven't already.

3 Algebraic

Now we consider the p-adic numbers algebraically. Start with $\mathbb{Z}$, and fix a prime $p \in \mathbb{Z}$. Define

$$\mathbb{Z}_p = \varprojlim_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$$

with transition maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ being the projections.

Give $\mathbb{Z}_p$ the induced topology from the product topology. It is closed in the product topology (exercise), hence compact.

Proposition 8. *Let $U_i = p^i \mathbb{Z}_p$, and give $\mathbb{Z}_p$ the topology such that U_i is a neighborhood base of 0. This is the same topology as above.*

Proposition 9. *The ring $\mathbb{Z}_p$ is compact, and isomorphic to $\mathbb{Z}_p$ from above.*

Proof. An element of our new $\mathbb{Z}_p$ is a sequence $(a_n + p^{n+1}\mathbb{Z})$ such that $a_n \equiv a_{n-1} \bmod p^n$. The number a_0 is determined by an element of R. a_1 is such that $a_1 \equiv a_0 \bmod p$, so $a_1 = a_0 + pb_0$, hence $a_2 = a_0 + pa_1 + p^2 b_2$, etc. Since $U_i = p^i \mathbb{Z}_p$ is a neighborhood base of zero, the sequence $b_n p^n \to 0$, so this sequence converges. Since $\mathbb{Z}_p$ is an inverse limit, it's enough to define maps out of our previous $\mathbb{Z}_p$ to $\mathbb{Z}/p^n\mathbb{Z}$ for all n which must factor through the inverse limit. Then we check injective and surjective.

Let x be an element of $\mathbb{Z}_p$. Then □

More generally, if A is any ring, M is an A-module, and I is an ideal of A, the *I-adic completion* of A is the ring

$$\widehat{A} = \varprojlim_{n \geq 1} A/I^n,$$

adnd the *I-adic completion* of M is the $\widehat{A}$-module

$$\widehat{M} = \varprojlim M/I^n M.$$

There are even more general sorts of completions where you take a filtration of A by ideals that are not necessarily powers of some ideal. Read Atiyah-MacDonald.

4 Topological

Of immesurable importance to number theory are *local fields*. These are, simply enough, locally compact fields.

Theorem 10. *Let K be a local field. Then K is a finite extension of $\mathbb{Q}_p$, or a finite extension of $\mathbb{F}_q((t))$.*

To prove this, we start with some preliminaries.

Theorem 11. *Let G be a locally compact group. Then there is a Radon measure μ on G that is left-invariant, i.e.*

$$\mu(g \cdot E) = \mu(E) \ \ \forall g \in G, \forall E \text{ measurable.}$$

Such a measure is unique up to scaling.

Proof. Hard. See any book on harmonic analysis. Better yet, read Ramakrishnan and Valenza's *Fourier Analysis on Number Fields.* □

This is called a *Haar measure* on G. Recall that a Radon measure is finite on compact sets, nonzero on open sets.

Let G be a locally compact abelian group, and $\alpha : G \to G$ be a continuous automorphism. If E is any Borel set, so is αE, so $\mu \circ \alpha$ is a Haar measure on G, so it's a multiple of μ; we call this multiple the *module of α*;

$$\mu(\alpha E) = \operatorname{mod}_G(\alpha)\mu(E).$$

Clearly

$$\operatorname{mod}_G(\alpha\beta) = \operatorname{mod}_G(\alpha)\operatorname{mod}_G(\beta).$$

Proposition 12. *Let K be a locally compact field with Haar measure μ. Then $\operatorname{mod}_K : K \to \mathbb{R}_{>0}$ is continuous.*

Proof. Fix a compact neighborhood E of zero and choose $a \in k$. Then $\mu(E) > 0$. Since μ is outer regular, for every $\varepsilon > 0$, there is some open set U such that $aK \subset U$ and

$$\mu(U) \leq \mu(aK) + \varepsilon.$$

Since multiplication is continuous and E is compact, there is a neighborhood W of a such that $WE \subset U$. But then for all $b \in W$, $bE \subset U$, so

$$\mu(bE) \leq \mu(aE) + \varepsilon$$

whence dividing by $\mu(E)$,

$$\mathrm{mod}_k(b) \leq \mathrm{mod}_k(a) + \mu(E)^{-1}\varepsilon.$$

Hence mod_k is continuous at zero. Moreover, it shows that the inverse image of $(0, x)$ is open. Since $\mathrm{mod}_k(a^{-1}) = \mathrm{mod}_k(a)^{-1}$, so the inverse image of (x, ∞) is open. Thus the inverse image of any interval is open, and we win. □

Corollary 13. *Assume k is nondiscrete. Let U be any neighborhood of zero.*

(a) *Then for every $\varepsilon > 0$, there is some $a \in U$ such that $0 < \mathrm{mod}_k(a) < \varepsilon$.*

(b) mod_k *is unbounded, so k is not compact.*

Proof. (a) We have that $\mathrm{mod}_k^{-1}[0, \varepsilon)$ is open, hence its intersection with U is a neighborhood of zero. So it contains a nonzero element a, (since U is nondiscrete), which has the desired property.

(b) By (a), there is a such that $0 < \mathrm{mod}_k(a) < \varepsilon$. Taking the inverse, we find that $\mathrm{mod}_k(a^{-1}) \geq \varepsilon^{-1}$. □

Proposition 14. *Let k be as above and $m \geq 1$ an integer. Then*

$$B_m = \{a \in k \,:\, \mathrm{mod}_k(a) \leq m\}$$

is compact.

Proof. Note that B_m is closed by continuity of mod_k. Let V be a compact neighborhood of zero, and let W be a neighborhood of zero such that $WV \subset V$. Then by the first corollary, there is some $r \in W \cap V$ with $0 < \mathrm{mod}_k(r) < 1$. Hence $r^n \in V$ for all $n \geq 1$, whence the sequence $\{r^n a\}$ for $a \in k$ lies in the compact set Va, and therefore has a limit point. But $\mathrm{mod}_k(r^n a) \to 0$, so the limit point is zero. Since V contains a neighborhood of zero, either $a \in V$ or $v_a := \min\{n \,:\, r^n a \in V\}$ is finite and positive. In the latter case, $r^{v_a} a \in V - rV$.

We claim that for $a \in B_m - V$, the v_a are bounded above. Granting this, it follows that B_m is contained in the union of the compact subsets $V, r^{-1}V, \ldots, r^{-M}V$ and is therefore compact.

Now let's prove the claim. Let X be the closure of $V - rV$, which is compact and excludes zero. Set

$$\beta = \inf_{x \in X} \mathrm{mod}_k(x).$$

Then $\beta > 0$, since a continuous function on a compact set achieves its minimum, which in this case cannot be zero. Choose M such that $\mathrm{mod}_k(r)^M < \beta/m$. Then if $a \in B_m - V$, we have

$$\mathrm{mod}_k(r)^M m \leq \beta \leq \mathrm{mod}_k(r)^{v_a} \,\mathrm{mod}_k(a) \leq \mathrm{mod}_k(r)^{v_a} \cdot m.$$

Since $0 < \mathrm{mod}_k(r) < 1$, we must have $v_a \leq M$. □

Corollary 15. *For $a \in k$, $\lim a^n = 0$ iff $\mathrm{mod}_k(a) < 1$.*

Proof. If $\mathrm{mod}_k(a) < 1$, then the a^n lie in the compact set B_1 and therefore $\{a^n\}$ converges. By continuity, the limit has module zero and is therefore also zero. Converse is trivial. □

Corollary 16. *Let F be a discrete field in k. Then for all $a \in F$, $\mathrm{mod}_k(a) = 1$. Moreover, F is finite.*

Proof. If $a \in F^\times$ but $\mathrm{mod}_k(a) < 1$, then $\{a^n\}$ lies in F which is not discrete, a contradiction. If $\mathrm{mod}_k(a) > 1$, same argument applies to a^{-1}. Moreover, discrete + compact implies finite. □

Proposition 17. *The sets B_r form a neighborhood base at zero for the topology of k.*

Proof. In a locally compact Hausdorff space, the compact neighborhoods of a point give a local base. On any compact neighborhood V of zero in k, mod_k is bounded, say by m. Hence $V \subset B_m$, and X the complement of the interior of V in B_m is likewise compact: set $\beta = \inf_{x \in X} \mathrm{mod}_k(x) > 0$. Then for any $0 < \gamma < \beta$, we have $B_\beta \subset V$. □

Proposition 18. *The function mod_k induces an open homomorphism of $k^\times$ onto a closed subgroup Γ of $\mathbb{R}_{>0}$.*

Proof. Let x be the limit of a sequence $\{\mathrm{mod}_k(a_j)\}$ with $a_j \in k$. The mod_k is bounded on this sequences, so eventually the a_j fall in a compact ball B_m. Hence x is in the closure of the continuous image of a compact set, which is itself compact, so $x \in \mathrm{mod}_k(B_m)$, so $\mathrm{mod}_k(k^\times)$ is closed.

Now we show that mod_k is open on $k^\times$. Let U denote the kernel of the restricted map, so we have a short exact sequence

$$1 \to U \to k^\times \to \Gamma \to 1.$$

Let V be an open subset of $k^\times$ and let $\{x_j\}$ be an sequence in Γ converging to some $x \in \mathrm{mod}_k(V)$. Set $x = \mathrm{mod}_k(a)$ for some $a \in V$. The sequences $\{x_j\}$ pulls back via mod_k to a sequence $\{a_j\}$ in the unit group $k^\times$, so the points eventually fall into one of the compact balls B_m. Therefore some subsequence $\{a'_j\}$ of the sequence $\{a_j\}$ converges, say to $\alpha \in k^\times$. By continuity, $\mathrm{mod}_k(\alpha) = x$, so $\alpha \in aU \subset VU$. Since VU is open, the points of $\{a'_j\}$ must eventually lie in VU. But $\mathrm{mod}_k(VU) = \mathrm{mod}_k(V)$, showing that the subsequence $\{\mathrm{mod}_k(a'_j)\}$ of the original sequence $\{x_j\}$, hence the entire sequence, eventually lands in $\mathrm{mod}_k(V)$. Hence the image of V is open. □

Theorem 19. *Let k be a locally compact indiscrete topological field with Haar measure μ. Then*

1. *There is a constant $A \geq 1$ such that*

$$\mathrm{mod}_k(a + b) \leq A \max\{\mathrm{mod}_k(a), \mathrm{mod}_k(b)\} \ \forall a, b \in k.$$

2. *If $A = 1$, then $\mathrm{mod}_k(k^\times)$ is discrete.*

Proof. Set $A = \sup_{b \in B_1} \mathrm{mod}_k(1 + b)$. The supremum is taking over a compact set (a translate of B_1), so A is finite and ≥ 1. Now consider $ab \neq 0$ and WLOG $\mathrm{mod}_k(b) \leq \mathrm{mod}_k(a)$. Setting $c = a^{-1}b$, $\mathrm{mod}_k(c) \leq 1$ and $a + b = a(1 + c)$; $\mathrm{mod}_k(1 + c) \leq A$, hence

$$\begin{aligned} \mathrm{mod}_k(a + b) &= \mathrm{mod}_k(a)\,\mathrm{mod}_k(1 + c) \\ &\leq A\,\mathrm{mod}_k(a) \\ &= A \max\{\mathrm{mod}_k(a), \mathrm{mod}_k(b)\}. \end{aligned}$$

If $A = 1$, let U be the interior of B_1. Then $\mathrm{mod}_k : 1 + U$ to an open subset of Γ containing 1 and contained in $[0, 1]$. Hence $\mathrm{mod}_k(1 + U)$ is the intersection of an open subset of $\mathbb{R}$ with Γ, so there is an open interval I containing 1 whose intersection with Γ is contained in $[0, 1]$. But 1 is a left accumulation point in Γ if and only if it is a right accumulation point (since $\mathrm{mod}_k(a^{-1}) = \mathrm{mod}_k(a)^{-1}$). Hence 1 must be open so Γ is discrete. □

Lemma 2. *If $F : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ is completely multiplicative and $F(m+n) \leq A \max\{F(m), F(n)\}$ for all m, n, then either (i) $F(m) \leq 1$ for all m or $F(m) = m^\lambda$ for some $\lambda > 0$.*

Proof. Exercise for the analytic number theorists in the room. Use log? □

Proposition 20. *If mod_k is bounded on the image of $\mathbb{Z}$, then $\mathrm{mod}_k \leq 1$ on the prime ring and k is ultrametric.*

Proof. We have $\mathrm{mod}_k(m^j) = \mathrm{mod}_k(m)^j$, so the induced map is bounded only if it lands in $[0, 1]$. It remains to show that k is ultrametric. Let $N = 2^n$. Then splitting the summation $\sum_{j=1}^N a_j$ into two sums containing half the terms, we have

$$\mathrm{mod}_k(\sum_{j=1}^N a_j) \leq A^n \sup_j \{\mathrm{mod}_k(a_j)\}.$$

hence

$$\mathrm{mod}_k(\sum_{j=1}^N a_j) \leq A^{\log_2(N)} \sup_j\{\mathrm{mod}_k(a_j)\}.$$

Thus

$$\mathrm{mod}_k(a+b)^{2^n} \leq A^{n+1} \sup_{0 \leq j \leq 2^n} \{\mathrm{mod}_k \binom{2^n}{j} \mathrm{mod}_k(a)^j \, \mathrm{mod}_k(b)^{2^n - j}\}.$$

Take logs, divide by 2^n, let n go to ∞, hence $\mathrm{mod}_k(a+b) \leq \mathrm{mod}_k(a)$. □