Convergence in $\mathbb{Q}_p$

Let a_i, b_{ij} etc. be elements of $\mathbb{Q}_p$

Recall: $\sum_{i\geq 0} a_i$ converges in $\mathbb{Q}_p$ (i.e. the sequence of $\sum_{i=0}^{n} a_i \in \mathbb{Q}_p$ converges)

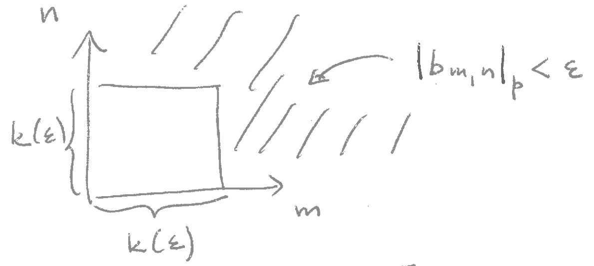
$$\Updownarrow$$

$\lim_{n\to\infty} a_n = 0$ in $\mathbb{Q}_p$ ($\Leftrightarrow \lim_{n\to\infty} |a_n|_p = 0$ in $\mathbb{R} \Leftrightarrow \lim_{n\to\infty} v_p(a_n) = +\infty$).

Cor: If $\sum_{n\geq 0} a_n$ and $\sum_{n\geq 0} b_n$ converge $\Rightarrow \sum_{n\geq 0}(a_n+b_n)$ converges to $\left(\sum_{n\geq 0} a_n\right) + \left(\sum_{n\geq 0} b_n\right)$.

Prop. Assume that $(b_{m,n})_{m,n\geq 0}$ in $\mathbb{Q}_p$ satisfy

(*) $\forall \varepsilon > 0\ \exists k(\varepsilon)$ such that $|b_{m,n}|_p < \varepsilon$ whenever $\max(m,n) \geq k(\varepsilon)$.



Then: (1) Every column $\sum_{n\geq 0} b_{m,n}$ converges

(2) Every row $\sum_{m\geq 0} b_{m,n}$ converges

(3) the sums $\sum_{m\geq 0}\left(\sum_{n\geq 0} b_{m,n}\right)$, $\sum_{n\geq 0}\left(\sum_{m\geq 0} b_{m,n}\right)$ converge to the same limit.

Pf. Exercise.

Cor. If $\sum_{i\geq 0} a_i$ and $\sum_{j\geq 0} b_j$ converge, then $\sum_{k\geq 0} c_k$ (where $c_k = \sum_{i+j=k} a_i b_j$) converges to $\left(\sum_{i\geq 0} a_i\right)\left(\sum_{j\geq 0} b_j\right)$.

Power series. Write $A(X) = \sum_{n\geq 0} a_n X^n$, $B(X) = \sum_{n\geq 0} b_n X^n$. If $C(X) = \sum_{n\geq 0} c_n X^n$, then is a formal product $C(X) = A(X)B(X)$.

Prop. (1) For $x \in \mathbb{Q}_p$, $A(x) := \sum_{n\geq 0} a_n x^n$ converges $\Longleftrightarrow \lim_{n\to\infty} |a_n|_p |x|_p^n = 0$.

In particular, if $0 < r \in \mathbb{R}$ and $\lim_{n\to\infty} |a_n|_p r^n = 0$, then $A(x)$ converges for all $x \in \mathbb{Q}_p$ with $|x|_p \leq r$.

(2) If $x \in \mathbb{Q}_p$ and if $A(x)$, $B(x)$ converge, so do $\sum (a_n+b_n)x^n$ and $C(x)$, and their respective limits are $A(x)+B(x)$ and $C(x)$.

The binomial series $\sum_{n\geq 0} \binom{a}{n} X^n$ in $\mathbb{Z}_p$

Note: For $n \in \mathbb{N}_+$, the polynomial $a \longmapsto \binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!}$ defines a continuous function $\mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ sending $a \in \mathbb{N}$ to $\binom{a}{n} \in \mathbb{N}$. As $\mathbb{N}$ is dense in $\mathbb{Z}_p$, $\binom{a}{n} \in \mathbb{Z}_p \ \forall a \in \mathbb{Z}_p$.

Cor. For each fixed $a \in \mathbb{Z}_p$, the power series

$$f_a(X) := \sum_{n\geq 0} \binom{a}{n} X^n \quad \text{converges at } x \in \mathbb{Q}_p \text{ if } \underbrace{|x|_p < 1}_{x \in p\mathbb{Z}_p}$$

(and $|f_a(x) - 1|_p < 1$)

Note: $\forall n \in \mathbb{N}_+$

$$\binom{a+b}{n} = \sum_{\substack{k+l=n \\ k,l\geq 0}} \binom{a}{k}\binom{b}{l} \quad \text{(as a polynomial identity in } \mathbb{Q}[\underbrace{a,b}_{\text{variables}}])$$

(if $a, b \in \mathbb{N}$, then $f_a(X) = (1+X)^a$, $f_b(X) = (1+X)^b$ and $f_{a+b}(X) = f_a(X) f_b(X)$, as polynomials in $\mathbb{Z}[X]$)

$$\Longrightarrow \forall a,b \in \mathbb{Z}_p \quad \underbrace{f_a(X) f_b(X)}_{\text{formal product of power series}} = f_{a+b}(X) \in \mathbb{Z}_p[[X]]$$

$$\Longrightarrow \forall a,b \in \mathbb{Z}_p \quad \forall x \in \mathbb{Q}_p \quad |x|_p < 1 \quad f_a(x) f_b(x) = f_{a+b}(x).$$

Cor: If $a, b \in \mathbb{Z}$, $b \geq 1$, $p \nmid b$, $x \in \mathbb{Q}_p$, $|x|_p < 1$

$$\Longrightarrow (f_{a/b}(x))^b = f_a(x) = (1+x)^a$$

Ex: $p = 7$, $\frac{a}{b} = \frac{1}{2}$, $1 + x = \frac{16}{9}$, $x = \frac{7}{9} \in 7\mathbb{Z}_7$. The value

$$y := f_{\frac{1}{2}}\left(\tfrac{7}{9}\right) = 1 + \underbrace{\sum_{n\geq 1} \binom{1/2}{n} \left(\tfrac{7}{9}\right)^n}_{\text{converges to an element of } 1+7\mathbb{Z}_7} \in 1 + 7\mathbb{Z}_7 \quad \text{satisfies}$$

$$\left.\begin{array}{l} \underbrace{y^2 = \frac{16}{9} \in \mathbb{Z}_{(7)} \subset \mathbb{Z}_7 \text{ and}} \quad y \equiv 1 \pmod{7\mathbb{Z}_7} \\ \Longrightarrow y = \pm\frac{4}{3} \in \mathbb{Z}_{(7)} \subset \mathbb{Z}_7 \end{array}\right\} \Longrightarrow \underline{y = -\frac{4}{3} \in \mathbb{Z}_{(7)} \subset \mathbb{Z}_7.}$$

On the other hand, the series

$$1 + \sum_{n\geq 1} \binom{1/2}{n} \left(\tfrac{7}{9}\right)^n \quad \text{also converges in } \mathbb{R},$$

to $y_{\mathbb{R}} > 0$ satisfying $y_{\mathbb{R}}^2 = \frac{16}{9} \in \mathbb{Q} \subset \mathbb{R} \Longrightarrow \underline{y_{\mathbb{R}} = 4/3 \in \mathbb{Q} \subset \mathbb{R}}.$

Exercise. Construct another example of this kind.

Formal composition of power series does <u>not</u> commute with evaluation (in general)!!

If $A(X) = \sum_{n\geq 0} a_n X^n$ and $B(X) = \sum_{n \geq 1} b_n X^n$ $\quad (a_n, b_n \in \mathbb{Q}_p,\ b_0 = B(0) = 0)$,

the coefficients d_n of the formal composition

$$D(X) = \sum_{n\geq 0} d_n X^n = A(B(X)) := \sum_{k \geq 0} a_k \Big(\sum_{\ell \geq 1} b_\ell X^\ell \Big)^k$$

are polynomial expressions (with coefficients in $\mathbb{Z}$) of $a_0, \ldots, a_n, b_1, \ldots, b_n$.

(!) <u>Warning</u>: if $x \in \mathbb{Q}_p$ and if $B(x)$ and $A(B(x))$ converge, it does <u>not</u> necessarily follow that $A(B(x))$ is equal to $D(x)$.

<u>Ex</u>: (related to the "Dwork exponential")

$p = 2$, $\quad A(X) = \sum_{n \geq 0} \frac{(4X)^n}{n!}$ $\quad$ ("$\exp(4X)$"), $\quad B(X) = \frac{X^2 - X}{2}$

$B(1) = 0$, $\quad A(B(1)) = A(0) = 1$

But $\quad D(X) = A(B(X)) = 1 - 2X + \sum_{n \geq 2} d_n X^n$ with

$\forall n \geq 2 \quad d_n \in 4\mathbb{Z}_2 \quad \Longrightarrow D(1) \in -1 + 4\mathbb{Z}_2 \Longrightarrow D(1) \neq A(B(1))$.

<u>Thm</u>. If $x \in \mathbb{Q}_p$, if $B(x)$ converges to $y \in \mathbb{Q}_p$, if $A(y)$ converges and if $\forall n \geq 1 \quad |b_n x^n|_p \leq |B(x)|_p$ $\quad \Longrightarrow \quad A(B(x)) = D(x)$.

Structure of $\mathbb{Z}_p^\times$ $\quad (p = \text{prime})$

$$\mathbb{Z}_p = \varprojlim_n \left(\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \cdots \leftarrow \mathbb{Z}/p^n\mathbb{Z} \leftarrow \cdots \right)$$

$$\mathbb{Z}_p^\times = \varprojlim_n \left((\mathbb{Z}/p\mathbb{Z})^\times \leftarrow (\mathbb{Z}/p^2\mathbb{Z})^\times \leftarrow \cdots \leftarrow (\mathbb{Z}/p^n\mathbb{Z})^\times \leftarrow \cdots \right)$$

pr_n

$$(1+p\mathbb{Z}_p, \cdot) = \varprojlim_n \left(\underbrace{\{1\}}_{Ker(pr_1)} \leftarrow \underbrace{1+p\mathbb{Z} \,(\mathrm{mod}\, p^2)}_{Ker(pr_2)} \leftarrow \cdots \leftarrow \underbrace{1+p\mathbb{Z}\,(\mathrm{mod}\, p^n)}_{Ker(pr_n)} \leftarrow \cdots \right)$$

Set $\underline{\delta := \begin{Bmatrix} 0 & p \neq 2 \\ 1 & p = 2 \end{Bmatrix}}$. Fix $\boxed{\begin{matrix} b = (b_n) \in 1+p^{1+\delta}\mathbb{Z}_p & \quad b_n \in 1+p^{1+\delta}\,(\mathrm{mod}\, p^n) \\ \notin 1+p^{2+\delta}\mathbb{Z}_p & \end{matrix}}$

<u>Exponential isomorphisms:</u>

$$(p^k\mathbb{Z}/p^n\mathbb{Z}, +) \xrightarrow{\sim} 1+p^{1+\delta+k}\mathbb{Z}\,(\mathrm{mod}\, p^{n+1+\delta}) \qquad (0 \leq k \leq n)$$

$$\exp_{b_{n+1+\delta}} : (\mathbb{Z}/p^n\mathbb{Z}, +) \xrightarrow{\sim} 1+p^{1+\delta}\mathbb{Z}\,(\mathrm{mod}\, p^{n+1+\delta}), \quad x\,(\mathrm{mod}\, p^n) \mapsto b_{n+1+\delta}^x\,(\mathrm{mod}\, p^{n+1+\delta})$$

$$\exp_{b_{n+2+\delta}} : (\mathbb{Z}/p^{n+1}\mathbb{Z}, +) \xrightarrow{\sim} 1+p^{1+\delta}\mathbb{Z}\,(\mathrm{mod}\, p^{n+2+\delta})$$

can pass to $\varprojlim_n$; obtain an isomorphism between the additive group of $\mathbb{Z}_p$ and an open subgroup of the multiplicative group $\mathbb{Z}_p^\times$:

$$\exp_b : \underbrace{\left(\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}, +\right)}_{(\mathbb{Z}_p, +)} \xrightarrow{\sim} \underbrace{\varprojlim_n 1+p^{1+\delta}\mathbb{Z}\,(\mathrm{mod}\, p^{n+1+\delta})}_{(1+p^{1+\delta}\mathbb{Z}_p, \cdot)} \cancel{= (1+p^{1+\delta}\mathbb{Z}_p, \cdot)}$$

$$(p^k\mathbb{Z}_p, +) \xrightarrow{\sim} (1+p^{k+1+\delta}\mathbb{Z}_p, \cdot) \qquad \forall k \geq 0$$

$$\exp_b(x) = \exp_b((x_n)) = \left(b_{n+1+\delta}^{x_n}\,(\mathrm{mod}\, p^{n+1+\delta})\right) \qquad \text{“} \exp_b(x) = b^x \text{”}$$

<u>$p=2$:</u> $\begin{matrix} b \in 1+4\mathbb{Z}_2 \\ b \notin 1+8\mathbb{Z}_2 \end{matrix} \Longrightarrow \exp_b : (\mathbb{Z}_2, +) \xrightarrow{\sim} (1+4\mathbb{Z}_2, \cdot)$

$$(2^k\mathbb{Z}_2, +) \xrightarrow{\sim} (1+2^{k+2}\mathbb{Z}_2, \cdot) \qquad (k \geq 0)$$

$$\mathbb{Z}_2^\times = \overbrace{\{\pm 1\}}^{\mu_2(\mathbb{Z}_2)} \oplus (1+4\mathbb{Z}_2, \cdot)$$

$$\mathbb{Z}_2^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \cong \{\pm 1\}$$

~~Solution de l'exercice 2.~~

$\underline{p \neq 2}$: $\forall n \geq 1$

$$\begin{array}{c} (\mathbb{Z}/p\mathbb{Z})^\times \xleftarrow{\sim} \\ \uparrow pr_n \end{array}$$

$$(\mathbb{Z}/p^n\mathbb{Z})^\times = \underbrace{\underbrace{(\mathbb{Z}/p^n\mathbb{Z})^\times[p-1]}_{\{a \,(\mathrm{mod}\, p^n) \mid a^{p-1} \equiv 1 [p^n]\}}}_{\mu_{p-1}(\mathbb{Z}/p^n\mathbb{Z})} \oplus \underbrace{\underbrace{(\mathbb{Z}/p^n\mathbb{Z})^\times[p^{n-1}]}_{\mathrm{Ker}(pr_n)}}_{(1+p\mathbb{Z}\,(\mathrm{mod}\, p^n))}$$

$$\uparrow \qquad \Uparrow \qquad \uparrow$$

$$\boxed{(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mu_{p-1}(\mathbb{Z}/p^{n+1}\mathbb{Z}) \oplus (1+p\mathbb{Z}\,(\mathrm{mod}\, p^{n+1}))}$$

Can pass to $\varprojlim$: $\underset{n}{\varprojlim}$:

$$\underbrace{\varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times}_{} = \underbrace{\left(\varprojlim_n \mu_{p-1}(\mathbb{Z}/p^n\mathbb{Z})\right)}_{} \oplus \underbrace{\varprojlim_n (1+p\mathbb{Z}\,(\mathrm{mod}\, p^n))}_{}$$

$$\boxed{\mathbb{Z}_p^\times = \mu_{p-1}(\mathbb{Z}_p) \oplus (1+p\mathbb{Z}_p, \cdot)}$$

$$pr = (pr_n) \downarrow \qquad \swarrow \sim$$

$$(\mathbb{Z}/p\mathbb{Z})^\times$$

Inverting the isomorphisms $\mu_{p-1}(\mathbb{Z}/p^n\mathbb{Z}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times = \mu_{p-1}(\mathbb{Z}/p\mathbb{Z})$

we get compatible sections

$$\begin{tikzcd} (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r, bend left, "s_n"] \arrow[d, equal] & (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[l, "pr_n"] \\ (\mathbb{Z}/p\mathbb{Z})^\times \arrow[r, "s_{n+1}"] & (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \arrow[u] \end{tikzcd}$$

of pr_n (morphisms (injective) with $pr_n \circ s_n = id$, $\mathrm{Im}(s_n) = \mu_{p-1}(\mathbb{Z}/p^n\mathbb{Z})$)

and $s = (s_n) : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}_p^\times$, $pr \circ s = id$, $\mathrm{Im}(s) = \mu_{p-1}(\mathbb{Z}_p)$.

$\underline{\text{Formula for } s_n}$: $(\mathbb{Z}/p\mathbb{Z})^\times \xleftarrow{pr_n} (\mathbb{Z}/p^n\mathbb{Z})^\times$

$$\underline{\text{given}} \quad a \quad \leftarrow \cdots\cdots \quad \tilde{a}$$

choose $\tilde{a}$ such that

$\underline{a = pr_n(\tilde{a}) = \tilde{a}\,(\mathrm{mod}\, p)}$. Then $\boxed{s_n(a) := \tilde{a}^{p^{n-1}}} \in (\mathbb{Z}/p^n\mathbb{Z})^\times[p-1]$ depends only on a, not on $\tilde{a}$. As $s_n(a)^{p-1} = 1$, $\boxed{s_n(a) = \tilde{a}^{p^k} \quad \forall k \geq n-1}$

$\underline{\text{Formula for } s}$: $(\mathbb{Z}/p\mathbb{Z})^\times \xleftarrow{pr} \mathbb{Z}_p^\times$

$$\underline{\text{given}} \quad a \quad \leftarrow \cdots\cdots \quad \tilde{a}$$

choose $\tilde{a} \in \mathbb{Z}_p^\times$ such that $\tilde{a}\,(\mathrm{mod}\, p) = a$.

Then $s(a) = \lim_{k \to +\infty} \tilde{a}^{p^k}$ (this converges in $\mathbb{Z}_p$, and depends only on a).

$\underline{\text{Terminology}}$: $s(a) \in \mu_{p-1}(\mathbb{Z}_p)$ is the $\underline{\text{Teichmüller representative}}$ of $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

$\underline{\text{Summary } (p \neq 2)}$: Fix $\boxed{\begin{array}{l} b \in 1+p\mathbb{Z}_p \\ b \notin 1+p^2\mathbb{Z}_p \end{array}}$

$$\boxed{\begin{array}{l} \mathbb{Z}_p^\times = \mu_{p-1}(\mathbb{Z}_p) \oplus (1+p\mathbb{Z}_p, \cdot) \\ \downarrow \qquad \swarrow \sim \\ (\mathbb{Z}/p\mathbb{Z})^\times \end{array}}$$

$$\boxed{\begin{array}{ll} \exp_b : (\mathbb{Z}_p, +) \xrightarrow{\sim} (1+p\mathbb{Z}_p, \cdot) & \\ \qquad\quad \cup \qquad\qquad\qquad \cup & \\ \qquad (p^k\mathbb{Z}_p, +) \xrightarrow{\sim} (1+p^{k+1}\mathbb{Z}_p, \cdot) & (k \geq 0) \end{array}}$$

~~Solution de l'exercice 1~~

Structure of $\mathbb{Z}_p^{\times m}$ and $\mathbb{Q}_p^{\times m}$

Note: $\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p^\times \mid v(x) = 0\}$, $\mathbb{Q}_p^\times = \mathbb{Z}_p^\times \times p^{\mathbb{Z}} \Longrightarrow \mathbb{Q}_p^{\times m} = \mathbb{Z}_p^{\times m} \times p^{m\mathbb{Z}}$, $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times m} = \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times m} \ast \boxed{p^{\mathbb{Z}/m\mathbb{Z}}}$

1st Case $p \neq 2$:

$b \in 1 + p\mathbb{Z}_p$
$\notin 1 + p^2\mathbb{Z}_p$

$$\begin{tikzcd}
\mathbb{Z}_p^\times \arrow[d] & \mu_{p-1}(\mathbb{Z}_p) \oplus (1+p\mathbb{Z}_p,\cdot) \arrow[l, "\sim"'] \\
(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times &
\end{tikzcd}$$

$$\begin{tikzcd}
\text{"}b^x\text{"} \in (1+p\mathbb{Z}_p,\cdot) & \supset (1+p^2\mathbb{Z}_p,\cdot) & \supset \dots \\
x \in (\mathbb{Z}_p,+) \arrow[u, "\exp_b"] & \supset (p\mathbb{Z}_p,+) \arrow[u, "\wr"] & \supset \dots
\end{tikzcd}$$

Cor. (a) $\forall k \geq 0$

$$\mathbb{Z}_p^{\times p^k} \xleftarrow{\sim} \mu_{p-1}(\mathbb{Z}_p) \oplus (1+p^{k+1}\mathbb{Z}_p,\cdot), \qquad 1+p^{k+1}\mathbb{Z}_p \overset{\exp_b}{\underset{\wr}{\longleftarrow}} p^k\mathbb{Z}_p$$

$$\mathbb{Z}_p^\times / \mathbb{Z}_p^{\times p^k} \xleftarrow{\sim} \underbrace{(1+p\mathbb{Z}_p,\cdot)/(1+p^{k+1}\mathbb{Z}_p,\cdot)}_{1+p\mathbb{Z}\ (\mathrm{mod}\ p^{k+1})} \overset{\exp_b}{\underset{\wr}{\longleftarrow}} \mathbb{Z}/p^k\mathbb{Z}$$

(b) If $m \geq 1$, $p \nmid m$:

$$\begin{tikzcd}
\mathbb{Z}_p^{\times m} \arrow[d] & \mu_{p-1}(\mathbb{Z}_p)^m \oplus (1+p\mathbb{Z}_p,\cdot) \arrow[l, "\sim"'] \arrow[dl, "\sim"] \\
\mathbb{F}_p^{\times m} &
\end{tikzcd}, \qquad \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times m} \xrightarrow{\sim} \mathbb{F}_p^\times / \mathbb{F}_p^{\times m}$$

In other words, for $a \in \mathbb{Z}_p^\times$: $\left[\exists x \in \mathbb{Z}_p \ \ x^m = a \Longleftrightarrow \exists y \in \mathbb{F}_p \ \ y^m = \underbrace{a\ (\mathrm{mod}\ p)}_{a_1}\right]$

$a = (a_n)_{\geq 1}$, $a_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$

2nd Case $p = 2$:

$b \in 1 + 2^2\mathbb{Z}_2$
$\notin 1 + 2^3\mathbb{Z}_2$

$$\begin{tikzcd}
\mathbb{Z}_2^\times \arrow[d] & \{\pm 1\} \oplus (1+2^2\mathbb{Z}_2,\cdot) \arrow[l, "\sim"'] \arrow[dl, "\sim"] \\
(\mathbb{Z}/2^2\mathbb{Z})^\times &
\end{tikzcd}$$

$$\begin{tikzcd}
(1+2^2\mathbb{Z}_2,\cdot) & \supset (1+2^3\mathbb{Z}_2,\cdot) & \supset \dots \\
(\mathbb{Z}_2,+) \arrow[u, "\wr\ \exp_b"] & \supset (2\mathbb{Z}_2,+) \arrow[u, "\wr"] & \supset \dots
\end{tikzcd}$$

Cor. (a) $\forall k \geq 1$

$$\mathbb{Z}_2^{\times 2^k} = (1+2^{2+k}\mathbb{Z}_2,\cdot) \overset{\exp_b}{\underset{\wr}{\longleftarrow}} 2^k\mathbb{Z}_2$$

$$\mathbb{Z}_2^\times / \mathbb{Z}_2^{\times 2} \xleftarrow{\sim} \mathbb{Z}_2^\times / (1+2^{2+k}\mathbb{Z}_2,\cdot) = (\mathbb{Z}/2^{2+k}\mathbb{Z})^\times \overset{(id,\ \exp_b)}{\underset{\wr}{\longleftarrow}} \{\pm 1\} \times (\mathbb{Z}/2^k\mathbb{Z})$$

(b) If $m \geq 1$, $2 \nmid m$: $\mathbb{Z}_2^{\times m} = \mathbb{Z}_2^\times$

Ex: (1) $p \neq 2 \Longrightarrow$

$$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} = \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} \oplus p^{\mathbb{Z}/2\mathbb{Z}} = \{\overline{1}, \overline{u}, \overline{p}, \overline{pu}\} \quad \text{4 elements}$$

$$\mathbb{Z}_p^\times / \mathbb{Z}_p^{\times 2} \overset{\wr}{\underset{\left(\frac{\cdot}{p}\right)}{\longrightarrow}} \{\pm 1\}$$

$u = (u_n) \in \mathbb{Z}_p$ s.t. $u_1 \in \mathbb{F}_p^\times$, $\left(\frac{u_1}{p}\right) = -1$

$\overline{x} :=$ the class of $x \in \mathbb{Q}_p^\times$ in $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$

(2) $p = 2$:

$$\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2} = \mathbb{Z}_2^\times / \mathbb{Z}_2^{\times 2} \oplus 2^{\mathbb{Z}/2\mathbb{Z}} = \{\overline{\pm 1}, \overline{\pm 5}, \overline{\pm 2}, \overline{\pm 10}\} \quad \text{8 elements}$$

$$\mathbb{Z}_2^\times / \mathbb{Z}_2^{\times 2} \overset{\wr}{\longrightarrow} (\mathbb{Z}/2^3\mathbb{Z})^\times$$

Exercise (Another definition of $\exp_b(x)$ $\left(= "b^x"\right)$ for $b \in 1+p\mathbb{Z}_p$, $x \in \mathbb{Z}_p$; writing $b = 1+a$ and making sense of $(1+a)^x$ as $\sum_{k\geq 0} \binom{x}{k} a^k$)

Let $p =$ prime, $a \in p\mathbb{Z}_p$.

(1) For each $k \in \mathbb{N}_+$, the polynomial $Q_k(X) := \dfrac{X(X-1)\cdots(X-k+1)}{k!} \in \mathbb{Q}[X]$ ($Q_0(x) = 1$) satisfies $Q_k(\mathbb{Z}_p) \subset \mathbb{Z}_p$ [Hint: $\mathbb{N}$ is dense in $\mathbb{Z}_p$.]

(2) $\forall k \in \mathbb{N}_+$ $\displaystyle\sum_{\substack{i+j=k \\ i,j\geq 0}} Q_i(X)\,Q_j(Y) = Q_k(X+Y) \in \mathbb{Q}[X,Y]$.

(3) $\forall x \in \mathbb{Z}_p$ the limit $f_a(x) := \underbrace{\lim_{n\to+\infty} \sum_{k=0}^{n} Q_k(x)a^k}$ $\in \mathbb{Z}_p$ exists.

(i.e., $\sum_{k=0}^{\infty} Q_k(x)a^k$ converges in $\mathbb{Z}_p$)

(4) $\forall x,y \in \mathbb{Z}_p$ $f_a(x+y) = f_a(x)\,f_a(y)$; $f_a(x) \in 1 + ax\mathbb{Z}_p$; $\forall z \in \mathbb{Z}$ $f_a(z) = (1+a)^z$.

(5) $\forall x,y \in \mathbb{Z}_p$ $v_p(f_a(x) - f_a(y)) \geq v_p(x-y) + v_p(a)$

($\Longleftrightarrow$ $|f_a(x) - f_a(y)|_p \leq |x-y|_p \cdot |a|_p$)

One writes, usually, $(1+a)^x$ instead of $f_a(x)$ ($a \in p\mathbb{Z}_p$, $x \in \mathbb{Z}_p$).

Rmk on adèles

let $f(x_1, \dots, x_M) \in \mathbb{Z}[x_1, \dots, x_M]$.

We know: $\forall n \geq 1$ $f \equiv 0\ [n]$ has a solution with $x_1, \dots, x_M \in \mathbb{Z}/n\mathbb{Z}$

$$\Updownarrow$$

$\forall p \in \mathcal{P}$ $\underbrace{\forall r \geq 1 \quad f \equiv 0\ [p^r] \text{ — '' — } \in \mathbb{Z}/p^r\mathbb{Z}}$

$\Updownarrow \longleftarrow$ (uses compactness of $\mathbb{Z}_p$)

$\forall p \in \mathcal{P}$ $f = 0$ has a solution with $x_1, \dots, x_M \in \mathbb{Z}_p$

$$\Updownarrow$$

$f = 0$ ——— '' ——— $\in \prod_p \mathbb{Z}_p =: \hat{\mathbb{Z}}$

Fact: $\hat{\mathbb{Z}} = \varprojlim_{m|n} \mathbb{Z}/n\mathbb{Z}$ (indexed by $(\mathbb{N}_+$, divisibility order$)$)

$= \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Z}/n\mathbb{Z},\ \forall m|n \quad x_n \equiv x_m\ [m]\}$

So: $f = 0$ has a solution with $x_1, \dots, x_M \in \mathbb{Z}$ $\ni a$

$\Downarrow$ $\quad \cap \quad$ $\downarrow$ diagonal map

——— '' ——— $\in \mathbb{R} \times \prod_p \mathbb{Z}_p = \mathbb{R} \times \hat{\mathbb{Z}}$ $\quad (a, a, a, \dots)$

Rings of interest:

$$\begin{array}{ccccc}
\mathbb{Z} & \subset & \mathbb{R} \times \hat{\mathbb{Z}} & \subset & \mathbb{R} \times \prod_p \mathbb{Z}_p \\
\cap & & \cap & & \cap \\
\mathbb{Q} = \bigcup_{m \geq 1} \frac{1}{m}\mathbb{Z} & \subset & \bigcup_{m \geq 1} \mathbb{R} \times \underbrace{\frac{1}{m}\hat{\mathbb{Z}}}_{\prod_p \frac{1}{m}\mathbb{Z}_p} & \subset & \underbrace{\mathbb{R} \times \prod_p \mathbb{Q}_p}_{\text{too big}}
\end{array}$$

(Def: $\underbrace{\hat{\mathbb{Q}}}_{\mathbb{A}^f_{\mathbb{Q}}} := \bigcup_{m \geq 1} \frac{1}{m}\hat{\mathbb{Z}} = \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ finite adèles)

$\mathbb{A}_{\mathbb{Q}} := \mathbb{R} \times (\hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q})$ adèles of $\mathbb{Q}$

$\mathbb{Q} \subset \mathbb{A}_{\mathbb{Q}} = \{x = (x_\infty; x_p)_{p \in \mathcal{P}} \mid x_\infty \in \mathbb{R},\ x_p \in \mathbb{Q}_p;$ for all but finitely many p $x_p \in \mathbb{Z}_p\}$

$\uparrow$
diagonal map

$=$ the subring of $\mathbb{R} \times \prod_p \mathbb{Q}_p$ generated by $\mathbb{Q}$ and $\mathbb{R} \times \prod_p \mathbb{Z}_p$

So: let $f(x_1, \dots, x_M) \in \mathbb{Q}[x_1, \dots, x_M]$.

$f = 0$ has a solution with $x_1, \dots, x_M \in \mathbb{Q}$
(global solution) $\Downarrow$

——— '' ——— $\in \mathbb{A}_{\mathbb{Q}}$
(local solutions everywhere)

Exercise: $\hat{\mathbb{Q}} = \hat{\mathbb{Z}} + \mathbb{Q}$, $\hat{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$

$\mathbb{A}_{\mathbb{Q}}/\mathbb{Q} = (\mathbb{R} \times \hat{\mathbb{Z}})/\mathrm{diag}(\mathbb{Z})$

$= \varprojlim_n \mathbb{R}/n\mathbb{Z}$

Question: when does "$\Uparrow$" hold? If yes, we say that the Hasse principle ("local-to-global principle") holds.

$\boxed{p = x^2+y^2 \quad - \quad \text{the descent method}}$

Prop. $p \equiv 1 \pmod 4$ prime $\Rightarrow \exists x, y \in \mathbb{Z} \quad x^2+y^2 = p$.

Pf: (Euler) —— " —— $\Rightarrow \exists a, b \in \mathbb{Z}, \quad 0 \le a < p/2, \quad a^2+1 = pb \quad (\Rightarrow 1 \le b < p/4)$

basic identity: if $\alpha = x+iy$, $\alpha' = x'+iy'$, then $\alpha\overline{\alpha'} = (xx'+yy') + i(-xy'+yx')$

and $(x^2+y^2)(x'^2+y'^2) = \underbrace{(\alpha\overline{\alpha})}_{N(\alpha)}\underbrace{(\alpha'\overline{\alpha'})}_{N(\alpha')} = N(\alpha\overline{\alpha'}) = (xx'+yy')^2 + (-xy'+yx')^2$

basic congruence: if $\alpha' \equiv \alpha \pmod{m\,\mathbb{Z}[i]}$, then $\alpha' = \alpha + m\beta \quad (\beta \in \mathbb{Z}[i])$

and $\alpha\overline{\alpha'} = \alpha\overline{\alpha} + m\alpha\overline{\beta}$ and if $m \mid N(\alpha)$ $= N(\alpha) + m\alpha\overline{\beta} \equiv 0 \pmod{m\,\mathbb{Z}[i]} \Rightarrow \dfrac{\alpha\overline{\alpha'}}{m} \in \mathbb{Z}[i]$.

Assume: we are given $x, y \in \mathbb{Z}$, $x^2+y^2 = pm$, $p \nmid m$, $m > 1$

(e.g. $x = a$, $y = 1$, $m = b$)

construction of $x'', y'' \in \mathbb{Z}$ with $x''^2 + y''^2 = pm'$, $1 \le m' < m$:

write $\alpha = x+iy \in \mathbb{Z}[i]$ and take $\alpha' = x'+iy' \in \mathbb{Z}[i]$, $\alpha' \equiv \alpha \pmod{m\,\mathbb{Z}[i]}$

with small $x', y' \in \mathbb{Z}$: $\left\{ \begin{array}{l} x' \equiv x \pmod m \\ y' \equiv y \pmod m \end{array} \right.$ and $|x'|, |y'| \le \frac{m}{2}$ $\}$

$\Rightarrow \alpha' \ne 0$ (if $x' = y' = 0 \Rightarrow m^2 \mid pm \Rightarrow m = p$ – false). As above,

$\dfrac{\alpha\overline{\alpha'}}{m} = \underbrace{x''+iy''}_{\alpha''} \in \mathbb{Z}[i]$ (in concrete terms, $xx'+yy' \equiv x^2+y^2 \equiv 0 \pmod m$, $-xy'+yx' \equiv -xy+yx \equiv 0 \pmod m$)

and $x''^2 + y''^2 = \underbrace{\dfrac{N(\alpha)}{m}}_{p}\underbrace{\dfrac{N(\alpha')}{m}}_{m'}$, $\quad N(\alpha') = x'^2+y'^2 \equiv x^2+y^2 \equiv 0 \pmod m$, $\quad 1 \le N(\alpha') \le \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 \le \frac{m^2}{2}$

$\Rightarrow$ $1 \le m' \le \frac{m}{2} < m$. If we knew that $p \nmid m'$, then we could repeat the same procedure with $x''+iy''$ instead of $x+iy$.

For our initial choice $\alpha = x+iy = a+i$ we have $1 \le m = b < p/4 < p$, so we obtain $1 \le m' < m < p$ again ($\Rightarrow p \nmid m'$). We can, therefore, continue until we obtain $m' = 1 \Rightarrow$ Prop.

Exercise: p prime, $a \in \{\pm 2, 3\}$, $\left(\frac{a}{p}\right) = 1 \Rightarrow \exists x, y \in \mathbb{Z} \quad x^2 - ay^2 = p$

(by the same method)

Note: the inequalities used are precisely those which imply that $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[\sqrt{a}]$ in the Exercise) is a Euclidean domain with respect to $|N(\alpha)|$.

The four square Thm by the descent method

Thm (Lagrange) $\forall n \in \mathbb{N}_+ \ \exists x, y, z, t \in \mathbb{Z} \quad x^2+y^2+z^2+t^2 = n.$

Pf (Euler) One uses the identity

$$(x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2) = (x''^2+y''^2+z''^2+t''^2), \quad \text{where}$$

$$x'' = xx'+yy'+zz'+tt', \ y'' = -xy'+yx'-zt'+tz', \ z'' = -xz'+yt'+zx'-ty', \ t'' = -xt'-yz'+zy'+tx'$$

[Where does this formula come from? $q = x+iy+jz+kt \in \mathbb{H}$ quaternion ($ij=-ji=k$, $i^2=j^2=-1$), $\bar{q} = x-iy-jz-kt$, $N(q) = q\bar{q} = x^2+y^2+z^2+t^2$, $q\overline{q'} = q''$,
$N(q'') = N(q)\,N(\overline{q'}) = N(q)\,N(q')$]

Enough to consider, therefore, $n = p > 2$ prime. We know that
$\exists a, b, m \in \mathbb{Z}$ such that $0 \le a, b \le (p-1)/2$, $a^2+b^2+1^2+0^2 = pm$ ($\Rightarrow 1 \le m < p$)
($\Rightarrow p \nmid m$)

Assume, in general, that $\exists x, y, z, t \in \mathbb{Z}$, $x^2+y^2+z^2+t^2 = pm$, $1 < m < p$

- if $2 \mid m$: can assume $\left.\begin{array}{l} x \equiv y \pmod 2 \\ z \equiv t \pmod 2 \end{array}\right\} \Rightarrow \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 = p\,\frac{m}{2}.$
- if $2 \nmid m$: take $x', y', z', t' \in \mathbb{Z}$, $x' \equiv x \pmod m$, $z' \equiv z \pmod m$, $y' \equiv y \pmod m$, $t' \equiv t \pmod m$, $|x'|, |y'|, |z'|, |t'| < \frac{m}{2}$

(not all x', y', z', t' are zero, since $m^2 \nmid pm$). This implies that

$q'' = q\overline{q'}$ is divisible by m (which can also be checked by hand; e.g. $x'' \equiv x^2+y^2+z^2+t^2 \equiv 0 \pmod m$), hence

$$m^2 \mid N(q'') = \underbrace{N(q)}_{pm}\,N(q') \ \underset{p \text{ prime}}{\overset{1<m<p}{\Longrightarrow}} \ m \mid N(q'), \quad x'^2+y'^2+z'^2+t'^2 = mm',$$

$$\left(\frac{x''}{m}\right)^2 + \left(\frac{y''}{m}\right)^2 + \left(\frac{z''}{m}\right)^2 + \left(\frac{t''}{m}\right)^2 = pm'. \quad \text{But } mm' < 4\left(\frac{m}{2}\right)^2 \Rightarrow 1 \le m' < m < p$$

We repeat the argument until $m' = 1 \Rightarrow$ Thm.