0 Some basics of p-adic valuation

Let F be a field with a non-archimedean valuation v.

Lemma 0.1. For $x, y, t \in F$ such that $v(k) \geq 0$, we have $\min\{v(tx+y), v(x)\} = \min\{v(x), v(y)\}$.

Proof. If $v(y) < v(x)$, then $v(kx+y) = v(y + \text{valuation} > v(y)) = v(y)$, so both sides are equal to $v(y)$. If $v(y) \geq v(x)$, then $v(kx+y) \geq \min\{v(k)+v(x), v(y)\} \geq v(x)$, so both sides are equal to $v(x)$. $\square$

Lemma 0.2. Suppose that $\operatorname{char} k \neq 2$. Pick $k \in F$ such that $v(k) \geq 0$. Suppose that F contains a square root $\sqrt{k+2}$ of $k+2$ and a square root $\sqrt{k-2}$ of $k-2$, then we have

$$v_p\left(\frac{\pm\sqrt{k+2} \pm \sqrt{k-2}}{2}\right) = 0.$$

Proof. The quantities $\dfrac{\pm\sqrt{k+2} \pm \sqrt{k-2}}{2}$ are the roots of

$$x^4 - kx^2 + 1 = 0.$$

If $v_p(x) > 0$, then we have $v_p(x^4 - kx^2 + 1) = v_p(1 + (\text{valuation} > 0)) = 0$, impossible. If $v_p(x) < 0$, then we have $v_p(x^4 - kx^2 + 1) = v_p(x^4 + (\text{valuation} > v_p(x^4))) = 4v_p(x) < 0$, impossible. $\square$

Now suppose that F is of characteristic 0. We extend the p-adic valuation v_p over $\mathbb{Q}$ to F (which is always possible thanks to https://math.stackexchange.com/questions/4535894).

Lemma 0.3. If $v_p(x) > \dfrac{1}{p-1}$, then

$$v_p((1+x)^p - 1) = v_p(x) + 1.$$

Proof. We have

$$v_p\left(\binom{p}{i}x^i\right) = v_p\left(\binom{p}{i}\right) + iv_p(x) = iv_p(x) + 1, \quad 1 \leq i \leq p-1$$

and

$$v_p\left(\binom{p}{p}x^p\right) = pv_p(x),$$

so

$$v_p((1+x)^p - 1) = v_p\left(\binom{p}{1}x + (\text{valuation} > 1 + v_p(x))\right) = v(x) + 1.$$

$\square$

Lemma 0.4. Let $d \in \mathbb{Z}$, and suppose that p is an odd prime such that $p \nmid d$. Suppose that F contains a square root $\sqrt{d}$ of d, then we have $v_p(\mathbb{Q}(\sqrt{d})^\times) \in \mathbb{Z}$; in other words, the p-adic valuation of a nonzero element in $\mathbb{Q}(\sqrt{d})$ (as a subfield of F) is an integer.

Proof. WLOG suppose that F is complete (if not, take the completion), then $\mathbb{Q}_p \subset F$. The result is obvious if d is a quadratic residue modulo p (which means that $\sqrt{d} \in \mathbb{Q}_p$). If not, then by the uniqueness of extending the p-adic valuation over $\mathbb{Q}_p$ to an algebraic extension (see for example Theorem 4.8, p.131 of *Algebraic Number Theory* by Neukirch), we have

$$v_p(a + b\sqrt{d}) = \frac{1}{2}v_p(\mathrm{Nm}_{\mathbb{Q}_p(\sqrt{d})/\mathbb{Q}_p}(a + b\sqrt{d})) = \frac{1}{2}v_p(a^2 - b^2 d).$$

It suffices to show that $v_p(a^2 - b^2 d)$ is even. WLOG suppose that $a, b \in \mathbb{Z}$, not being divisible by p at the same time. If $p \mid (a^2 - b^2 d)$, then $a^{p-1} \equiv b^{p-1} d^{\frac{p-1}{2}} \equiv -b^{p-1} \pmod{p}$, which implies $p \mid a, b$, a contradiction. We obtain then that $v_p(a^2 - b^2 d) = 0$. $\square$

In the following sections, we will write $p^e \mid x$ for $x \in \mathbb{Q}(\sqrt{d})$ if $v_p(x) \geq e$. If $p^e \mid (x - y)$, we write $x \equiv y \pmod{p^e}$.

1 Lucas sequences and entry point modulo p

Let $k \geq 3$ be a fixed integer. Consider the sequence in $\mathbb{Q}(\sqrt{k-2})$ (an extension of $\mathbb{Q}$ that contains a square root $\sqrt{k-2}$) defined by

$$x_0 = 0, \quad x_1 = 1, \quad x_{n+2} = \sqrt{k-2}x_{n+1} + x_n, \quad \forall n \in \mathbb{N}.$$

(x_n) is an increasing sequence, so $x_n > 0$ for $n \in \mathbb{N}^*$. We have

$$x_n = \begin{cases} \dfrac{\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{2i+1}(k+2)^i(k-2)^{\frac{n-1}{2}-i}}{2^{n-1}}, & n \text{ odd;} \\ \sqrt{k-2}\,\dfrac{\sum_{i=0}^{\frac{n}{2}-1} \binom{n}{2i+1}(k+2)^i(k-2)^{\frac{n}{2}-1-i}}{2^{n-1}}, & n \text{ even,} \end{cases} \tag{1}$$

and in $\mathbb{Q}(\sqrt{k-2}, \sqrt{k+2})$ we have

$$x_n = \frac{\left(\frac{\sqrt{k-2}+\sqrt{k+2}}{2}\right)^n - \left(\frac{\sqrt{k-2}-\sqrt{k+2}}{2}\right)^n}{\sqrt{k+2}}.$$

We will always suppose henthforth that p **is an odd prime such that** $p \nmid k-2$, and we extend the p-adic valuation v_p over $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{k-2})$ and $\mathbb{Q}(\sqrt{k-2}, \sqrt{k+2})$.

Lemma 1.1. For $n, m \in \mathbb{N}$, we have $\min\{v_p(x_n), v_p(x_m)\} = v_p(x_{\gcd(n,m)})$.

Proof. By Lemma 0.1, we have

$$x_{m+1} = \sqrt{k-2}x_m + x_{m-1} \Rightarrow \min\{v_p(x_{m+1}), v_p(x_m)\} = \min\{v_p(x_m), v_p(x_{m-1})\}, \quad \forall m \in \mathbb{N}^*,$$

so $\min\{v_p(x_m), v_p(x_{m-1})\} = \cdots = \min\{v_p(x_1), v_p(x_0)\} = 0$, which means that $v_p(x_m) = 0$ or $v_p(x_{m-1}) = 0$ for all $m \in \mathbb{N}^*$. Now WLOG suppose that $n \geq m \geq 1$. By induction we have

$$x_n = x_m x_{n-m+1} + x_{m-1}x_{n-m},$$

so Lemma 0.1 gives

$$\min\{v_p(x_n), v_p(x_m)\} = \min\{v_p(x_m), v_p(x_{m-1}) + v_p(x_{n-m})\}.$$

But $v_p(x_m) = 0$ or $v_p(x_{m-1}) = 0$, so we obtain

$$\min\{v_p(x_n), v_p(x_m)\} = \min\{v_p(x_m), v_p(x_{n-m})\}.$$

After finitely many steps, we obtain

$$\min\{v_p(x_n), v_p(x_m)\} = \min\{v_p(x_{\gcd(n,m)}), v_p(x_0)\} = v_p(x_{\gcd(n,m)}).$$

□

In particular, if $n \mid m$ for $n, m \in \mathbb{N}$, then $v_p(x_m) \geq v_p(x_n)$.

By (1), $v_p(x_n)$ is always a nonnegative integer for $n \in \mathbb{N}^*$. Define

$$r := \min\{n \in \mathbb{N}^* : v_p(x_n) \geq 1\}.$$

By Lemma 1.1, we have $p \mid x_n \Leftrightarrow r \mid n$. The quantity r is called the **entry point of** (x_n) **modulo** p. The following property shows that r is well-defined.

Proposition 1.1. We have $p \mid x_{p-\left(\frac{k^2-4}{p}\right)}$, so $r \mid \left(p - \left(\frac{k^2-4}{p}\right)\right)$.

Proof. Since p is odd, (1) gives

$$\frac{x_{p+1}}{\sqrt{k-2}} = \frac{\sum_{i=0}^{\frac{p-1}{2}} \binom{p+1}{2i+1}(k+2)^i(k-2)^{\frac{p-1}{2}-i}}{2^p} \equiv \frac{(k-2)^{\frac{p-1}{2}} + (k+2)^{\frac{p-1}{2}}}{2} \pmod p;$$

$$\frac{x_{p-1}}{\sqrt{k-2}} = \frac{\sum_{i=0}^{\frac{p-3}{2}} \binom{p-1}{2i+1}(k+2)^i(k-2)^{\frac{p-3}{2}-i}}{2^{p-2}} \equiv \frac{-\sum_{i=0}^{\frac{p-3}{2}}(k+2)^i(k-2)^{\frac{p-3}{2}-i}}{2^{p-2}} \equiv \frac{(k-2)^{\frac{p-1}{2}} - (k+2)^{\frac{p-1}{2}}}{2} \pmod p;$$

$$x_p = \frac{\sum_{i=0}^{\frac{p-1}{2}} \binom{n}{2i+1}(k+2)^i(k-2)^{\frac{p-1}{2}-i}}{2^{p-1}} \equiv (k+2)^{\frac{p-1}{2}} \pmod p.$$

□

Proposition 1.2. If $p \nmid (k^2-4)$, then $r \mid \frac{p-\left(\frac{k^2-4}{p}\right)}{2}$ if and only if $\left(\frac{-(k-2)}{p}\right) = 1$.

Proof. We calculate $x_{\frac{p-1}{2}} x_{\frac{p+1}{2}}$ modulo p. Write $\alpha = \frac{\sqrt{k-2}+\sqrt{k+2}}{2}$, $\beta = \frac{\sqrt{k-2}-\sqrt{k+2}}{2}$ in $\mathbb{Q}(\sqrt{k-2}, \sqrt{k+2})$, then

$$\begin{aligned} x_{\frac{p-1}{2}} x_{\frac{p+1}{2}} &= \frac{(\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}})(\alpha^{\frac{p+1}{2}} - \beta^{\frac{p+1}{2}})}{k+2} = \frac{(\alpha^{\frac{p-1}{2}} - \beta^{\frac{p-1}{2}})(\alpha^{\frac{p+1}{2}} - \beta^{\frac{p+1}{2}})}{k+2} \\ &= \frac{\alpha^p + \beta^p - (-1)^{\frac{p-1}{2}}\sqrt{k-2}}{k+2} = \sqrt{k-2}\,\frac{\sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i}(k+2)^i(k-2)^{\frac{p-1}{2}-i} - (-1)^{\frac{p-1}{2}}}{k+2} \\ &\equiv \sqrt{k-2}\,\frac{(k-2)^{\frac{p-1}{2}} - (-1)^{\frac{p-1}{2}}}{k+2} \pmod p, \end{aligned}$$

so $p \mid x_{\frac{p-1}{2}} x_{\frac{p+1}{2}}$ if and only if $\left(\frac{-(k-2)}{p}\right) = 1$. If $\left(\frac{-(k-2)}{p}\right) = 1$, then we have $p \mid x_{\frac{p-1}{2}}$ or $p \mid x_{\frac{p-1}{2}}$ (since $v_p\left(x_{\frac{p-1}{2}}\right), v_p\left(x_{\frac{p+1}{2}}\right) \in \mathbb{N}$), but $r \mid \left(p - \left(\frac{k^2-4}{p}\right)\right)$, so $r \mid \frac{p-\left(\frac{k^2-4}{p}\right)}{2}$. If $\left(\frac{-(k-2)}{p}\right) = -1$, then p divides neither $x_{\frac{p-1}{2}}$ nor $x_{\frac{p-1}{2}}$, so $r \nmid \frac{p-\left(\frac{k^2-4}{p}\right)}{2}$. □

Conclusion. Let p be an odd prime such that $p \nmid (k^2-4)$.

(1) $\left(\frac{-(k-2)}{p}\right) = 1$, $\left(\frac{k+2}{p}\right) = -1$.

Since r divides $\frac{p-\left(\frac{k^2-4}{p}\right)}{2} = \frac{p+\left(\frac{k^2-4}{p}\right)}{2}$, which is odd, r **must be odd**.

(2) $\left(\frac{-(k-2)}{p}\right) = -1$, $\left(\frac{k+2}{p}\right) = -1$.

Since r has the same number of factors 2 as $p - \left(\frac{k^2-4}{p}\right) = p - \left(\frac{-1}{p}\right)$, which is a mulitple of 4, r **must be divisible by** 4.

(3) $\left(\dfrac{-(k-2)}{p}\right)=-1$, $\left(\dfrac{k+2}{p}\right)=1$.

Since r has the same number of factors 2 as $p-\left(\dfrac{k^2-4}{p}\right)=p+\left(\dfrac{-1}{p}\right)$, which is congruent to 2 modulo 4, **we must have** $r\equiv 2\pmod 4$.

(4) $\left(\dfrac{-(k-2)}{p}\right)=1$, $\left(\dfrac{k+2}{p}\right)=1$, $\left(\dfrac{2}{p}\right)=1$ ($p\equiv 1,7\pmod 8$).

Conjecture: The relative densities of r odd, $r\equiv 2\pmod 4$ and $4\mid r$ is respectively $\dfrac{1}{6}$, $\dfrac{1}{6}$ and $\dfrac{2}{3}$.

(5) $\left(\dfrac{-(k-2)}{p}\right)=1$, $\left(\dfrac{k+2}{p}\right)=1$, $\left(\dfrac{2}{p}\right)=-1$ ($p\equiv 3,5\pmod 8$).

Since r divides $\dfrac{p-\left(\frac{k^2-4}{p}\right)}{2}=\dfrac{p-\left(\dfrac{-1}{p}\right)}{2}$, which is not divisible by 4, r cannot be divisible by 4.

Conjecture: The relative densities of r odd and $r\equiv 2\pmod 4$ is respectively $\dfrac{1}{2}$ and $\dfrac{1}{2}$.

Note that **if $\dfrac{k+2}{2}$ is a square, the last case cannot happen**. Under the conjectures,

- If $\dfrac{k+2}{2}$ is a square (cases (i)$-$(iv) with densities $\frac{1}{4}$, $\frac{1}{4}$, $\frac{1}{4}$, $\frac{1}{4}$), the relative densities of the three cases are $\frac{1}{4}\times 1+\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{4}\times\frac{1}{6}=\frac{7}{24}$, $\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{4}\times 1+\frac{1}{4}\times\frac{1}{6}=\frac{7}{24}$ and $\frac{1}{4}\times 0+\frac{1}{4}\times 1+\frac{1}{4}\times 0+\frac{1}{4}\times\frac{2}{3}=\frac{5}{12}$.
- If $k+2$ is a square (cases (iii)$-$(v) with densities $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{4}$), the relative densities of the three cases are $\frac{1}{2}\times 0+\frac{1}{4}\times\frac{1}{6}+\frac{1}{4}\times\frac{1}{2}=\frac{1}{6}$, $\frac{1}{2}\times 1+\frac{1}{4}\times\frac{1}{6}+\frac{1}{4}\times\frac{1}{2}=\frac{2}{3}$ and $\frac{1}{2}\times 0+\frac{1}{4}\times\frac{2}{3}+\frac{1}{4}\times 0=\frac{1}{6}$.
- In other cases (cases (i)$-$(v) with densities $\frac{1}{4}$, $\frac{1}{4}$, $\frac{1}{4}$, $\frac{1}{8}$, $\frac{1}{8}$), the relative densities of the three cases are $\frac{1}{4}\times 1+\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{8}\times\frac{1}{6}+\frac{1}{8}\times\frac{1}{2}=\frac{1}{3}$, $\frac{1}{4}\times 0+\frac{1}{4}\times 0+\frac{1}{4}\times 1+\frac{1}{8}\times\frac{1}{6}+\frac{1}{8}\times\frac{1}{2}=\frac{1}{3}$ and $\frac{1}{4}\times 0+\frac{1}{4}\times 1+\frac{1}{4}\times 0+\frac{1}{8}\times\frac{2}{3}+\frac{1}{8}\times 0=\frac{1}{3}$.

We will explain in the next section the reason why we are interested in the three cases r odd, $r\equiv 2\pmod 4$ and $4\mid r$.

2 Number of zeros in a period modulo p^e

Suppose that $p^e \mid x_s$ for some $s \in \mathbb{N}$. By recurrence we have

$$x_{n+s} \equiv x_{s+1} x_n \pmod{p^e} \tag{2}$$

(the expression makes sense by Lemma 0.4), so we are interested in $x_{s+1} \bmod p^e$. We have:

Lemma 2.1. $x_{s+1}^2 \equiv (-1)^s \pmod{p^e}$.

Proof. The result is obvious for $s = 0$. For $s > 0$, note that $p^e \mid x_s$ implies that $x_{s+1} \equiv x_{s-1} \pmod{p^e}$. Set $A = \begin{pmatrix} \sqrt{k-2} & 1 \\ 1 & 0 \end{pmatrix}$, then $A^n = \begin{pmatrix} x_{n+1} & x_n \\ x_n & x_{n-1} \end{pmatrix}$ for $n \in \mathbb{N}^*$, so

$$A^s \equiv x_{s+1} I_2 \pmod{p^e}.$$

Taking the determinant of both sides yields

$$x_{s+1}^2 \equiv \det(A)^s = (-1)^s \pmod{p^e}.$$

□

Lemma 2.2. If $v_p(x_n) > 0$ for some $n \in \mathbb{N}^*$, then $v_p(x_{pn}) = v_p(x_n) + 1$.

Proof. Write $\alpha = \dfrac{\sqrt{k-2} + \sqrt{k+2}}{2}$, $\beta = \dfrac{\sqrt{k-2} - \sqrt{k+2}}{2}$ in $\mathbb{Q}(\sqrt{k-2}, \sqrt{k+2})$, then by Lemma 0.2 we have

$$v_p(x_n) = v_p\left(\frac{\alpha^n - \beta^n}{\sqrt{k+2}}\right) = v_p\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) - v_p(\sqrt{k+2}),$$

so we have $v_p\left(\left(\dfrac{\alpha}{\beta}\right)^n - 1\right) \geq v_p(x_n) \geq 1$. By Lemma 0.3 we have

$$v_p\left(\left(\frac{\alpha}{\beta}\right)^{np} - 1\right) = v_p\left(\left(\frac{\alpha}{\beta}\right)^n - 1\right) + 1,$$

which means that $v_p(x_{pn}) = v_p(x_n) + 1$. □

Let

$$r_e := \min\{n \in \mathbb{N}^* : v_p(x_n) \geq e\};$$

since r_1 is well-defined, the quantity is well-defined thanks to the lemma above. By Lemma 1.1, we have $p^e \mid x_n \Leftrightarrow r_e \mid n$. By (2), the multiplicative order of x_{r_e+1} modulo p^e representes the number of zeros in a period of Lucas sequence modulo p^e. We have:

Proposition 2.1.

- If r_e is odd, then the multiplicative order of x_{r_e+1} is 4;
- If $r_e \equiv 2 \pmod 4$, then the multiplicative order of x_{r_e+1} is 1;
- If $4 \mid r_e$, then the multiplicative order of x_{r_e+1} is 2.

Proof. If r_e is odd, then $x_{r_e+1}^2 \equiv -1 \pmod{p^e}$ by Lemma 2.1, so the multiplicative order is 4. Suppose that r_e is even. Note the relation

$$x_{2n+1} = \frac{x_{n+1} x_{2n}}{x_n} - (-1)^n, \quad \forall n \in \mathbb{N}^*.$$

We claim that p does not divide $x_{\frac{r_e}{2}}$. If it does, then $p^e \mid x_{p^{e-1}\frac{r_e}{2}}$ by Lemma 2.2, so $r_e \mid p^{e-1}\frac{r_e}{2}$, or $2 \mid p^{e-1}$, which is impossible. Taking $n = \dfrac{r_e}{2}$ in the equation above yields

$$x_{r_e+1} \equiv -(-1)^{\frac{r_e}{2}} \pmod{p^e},$$

which is the desired result. □