Discriminants of iterated quadratic extensions

Alden Gassert

University of Colorado Boulder

January 8, 2016

JMM 2016

Iterated extensions

Setup:

- $f \in \mathbb{Z}[x]$ monic
- $\deg f = d \geq 2$
- $f^n(x) := f \circ \overset{n}{\cdots} \circ f$
- let $t \in \mathbb{Z}$ and fix a sequence of preimages of t:

$$\{\theta_0 = t, \theta_1, \theta_2, \ldots\}, \qquad f(\theta_n) = \theta_{n-1}.$$

Let $K_n = \mathbb{Q}(\theta_n)$. Assuming $f^n(x)$ is irreducible,

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots$$

is an infinite tower of fields; $[K_n : \mathbb{Q}] = d^n$.

Iterated quadratic extensions

Let $f(x) = x^2 + c$, $c \neq -1, -2$ is square-free.

What can be said about ramification in iterated extensions generated by $f^n(x)$?

Iterated quadratic extensions

Let $f(x) = x^2 + c$, $c \neq -1, -2$ is square-free.

What can be said about ramification in iterated extensions generated by $f^n(x)$?

Start with the discriminant of $f^n(x)$:

$$\operatorname{disc} f^n(x) = [\mathcal{O}_{K_n} : \mathbb{Z}[\theta_n]]^2 \operatorname{disc} K_n.$$

The discriminant of iterated maps is given by its critical orbits.

$$\operatorname{disc} f^n(x) = \pm 2^{n2^n} \prod_{k=1}^{n} \left(f^k(0) \right)^{2^{n-k}}.$$

Discriminant "lag" for $x^2 + 3$

n	$\operatorname{disc} f^n(x)$	$\operatorname{disc} K_n$
1	$-2^2\,3$	-3

Discriminant "lag" for $x^2 + 3$

n	$\operatorname{disc} f^n(x)$	$\operatorname{disc} K_n$
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$

Discriminant "lag" for $x^2 + 3$

n	$\operatorname{disc} f^n(x)$	$\operatorname{disc} K_n$
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$
3	$2^{28}\,3^7\,7^2$	$2^{20}\,3^7$

Discriminant "lag" for $x^2 + 3$

n	$\operatorname{disc} f^n(x)$	$\operatorname{disc} K_n$
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$
3	$2^{28}\,3^7\,7^2$	$2^{20}\,3^7$
4	$2^{74}\,3^{15}\,7^4\,1801$	$2^{58}\,3^{15}\,1801$

Discriminant "lag" for $x^2 + 3$

n	disc $f^n(x)$	disc K_n
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$
3	$2^{28}\,3^7\,7^2$	$2^{20}\,3^7$
4	$2^{74}\,3^{15}\,7^4\,1801$	$2^{58}\,3^{15}\,1801$
5	$2^{180}\,3^{31}\,7^8\,1801^2\,13 \cdot 3019 \cdot 3967$	$2^{148}\,3^{31}\,1801^2\,13 \cdot 3019 \cdot 3967$

Discriminant "lag" for $x^2 + 3$

n	disc $f^n(x)$	disc K_n
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$
3	$2^{28}\,3^7\,7^2$	$2^{20}\,3^7$
4	$2^{74}\,3^{15}\,7^4\,1801$	$2^{58}\,3^{15}\,1801$
5	$2^{180}\,3^{31}\,7^8\,1801^2\,13 \cdot 3019 \cdot 3967$	$2^{148}\,3^{31}\,1801^2\,13 \cdot 3019 \cdot 3967$
6	$2^{426}\,3^{63}\,7^{18}\,1801^4\,(13 \cdot 3019 \cdot 3967)^2\,p_1\,p_2$	$2^{362}\,3^{63}\,1801^4\,(13 \cdot 3019 \cdot 3967)^2\,7^2\,p_1\,p_2$

Discriminant "lag" for $x^2 + 3$

n	$\operatorname{disc} f^n(x)$	$\operatorname{disc} K_n$
1	$-2^2\,3$	-3
2	$2^{10}\,3^3$	$2^6\,3^3$
3	$2^{28}\,3^7\,7^2$	$2^{20}\,3^7$
4	$2^{74}\,3^{15}\,7^4\,1801$	$2^{58}\,3^{15}\,1801$
5	$2^{180}\,3^{31}\,7^8\,1801^2\,13\cdot 3019\cdot 3967$	$2^{148}\,3^{31}\,1801^2\,13\cdot 3019\cdot 3967$
6	$2^{426}\,3^{63}\,7^{18}\,1801^4\,(13\cdot 3019\cdot 3967)^2\,p_1\,p_2$	$2^{362}\,3^{63}\,1801^4\,(13\cdot 3019\cdot 3967)^2\,7^2\,p_1\,p_2$

Can we explain this phenomenon?

Are there any primes that appear in $\operatorname{disc} f^n$ for some n, but never ramify in the iterated tower?

Irreducibility of $f^n(x)$

Observe: $p \mid f^n(0)$ for some $n \Leftrightarrow 0$ is periodic modulo p.

Let

- m denote the exact period of 0 modulo p
- $\varphi(x) = f^m(x)$
- $k = \nu_p(\varphi(0))$.

Note: $\nu_p(\varphi^n(0)) = k$. (Rigid divisibility)

Irreducibility of $f^n(x)$

Observe: $p \mid f^n(0)$ for some $n \Leftrightarrow 0$ is periodic modulo p.

Let

- m denote the exact period of 0 modulo p
- $\varphi(x) = f^m(x)$
- $k = \nu_p(\varphi(0))$.

Note: $\nu_p(\varphi^n(0)) = k$. (Rigid divisibility)

$$\varphi(x) = \varphi(0) + a_2x^2 + a_4x^4 + \cdots$$
$$\varphi^2(0) = \varphi(\varphi(0)) = \varphi(0) + a_2\varphi(0)^2 + a_4\varphi^4(0) + \cdots$$

Irreducibility of $f^n(x)$

Observe: $p \mid f^n(0)$ for some $n \Leftrightarrow 0$ is periodic modulo p.

Let

- m denote the exact period of 0 modulo p
- $\varphi(x) = f^m(x)$
- $k = \nu_p(\varphi(0))$.

Note: $\nu_p(\varphi^n(0)) = k$. (Rigid divisibility)

$$\varphi(x) = \varphi(0) + a_2x^2 + a_4x^4 + \cdots$$
$$\varphi^2(0) = \varphi(\varphi(0)) = \varphi(0) + a_2\varphi(0)^2 + a_4\varphi^4(0) + \cdots$$

Thus if $c \neq 1$ is squarefree and $p \mid c$, then $f^n(x)$ is Eisenstein at p.
For $c = 1$, then use $f^2(x) = x^2 + 2x + 2$.

p-adic valuation of the index

Theorem: (G.) Set $\mathrm{ind}_p(\varphi^n) = \mathrm{ind}_p(f^{mn}) := \nu_p[\mathcal{O}_{K_{mn}} : \mathbb{Z}[\theta_{mn}]]$. Then for $p > 2$,

$$\mathrm{ind}_p(\varphi^n) = \frac{(2^{mn}-1)(k-1)}{2(2^m-1)} + \frac{\gcd(2^n,k)-1}{2} + \frac{1-2^{1-m}}{2}\sum_{i=1}^{n-1} 2^{im}(\gcd(2^{n-i},k)-1).$$

In particular, if k is odd, then

$$\mathrm{ind}_p(\varphi^n) = \frac{(2^{mn}-1)(k-1)}{2(2^m-1)}.$$

If k is even, set $v = \nu_2(k)$. Then

$$\mathrm{ind}_p(\varphi^n) = \frac{k(2^{mn}-1) - 2^v(2^{m(n-v)}-1)}{2(2^m-1)} \qquad \text{provided } n \geq v.$$

Condition for monogeneity

If $k = 1$ (i.e. $\nu_p(\varphi(0)) = 1$), then

$$\operatorname{ind}_p(\varphi^n) = \frac{(2^{mn} - 1)(k - 1)}{2(2^m - 1)} = 0.$$

If $\operatorname{ind}_p(\varphi^n) = 0$ for every p, then $\operatorname{disc} \varphi^n = \operatorname{disc} K_{mn}$.

Corollary: If $f(0), f^2(0), f^3(0), \ldots, f^n(0)$ are square-free, then $\mathcal{O}_{K_n} = \mathbb{Z}[\theta_n]$. That is, K_n is monogenic.

Montes algorithm (GMN 2009–2012)

Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.

Montes algorithm (GMN 2009–2012)

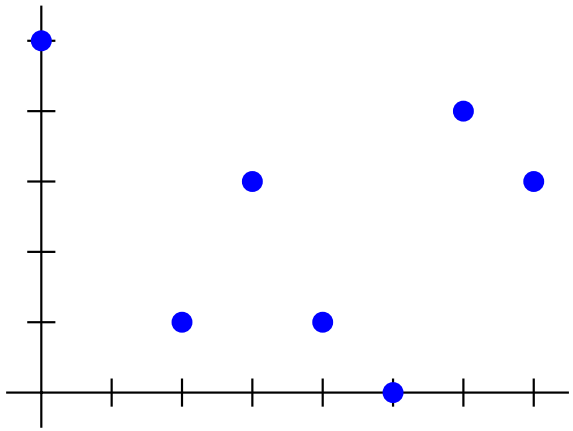
Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.
2) For each irreducible factor f_i, write
$f(x) = a_0(x) + a_1(x)f_i(x) + a_2(x)f_i(x)^2 + \cdots + a_g(x)f_i(x)^g$.

Montes algorithm (GMN 2009–2012)

Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.
2) For each irreducible factor f_i, write
$f(x) = a_0(x) + a_1(x)f_i(x) + a_2(x)f_i(x)^2 + \cdots + a_g(x)f_i(x)^g$.
3) Determine the f_i-polygon of f,

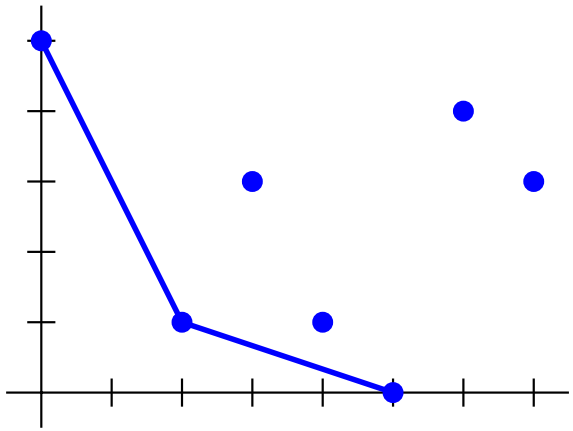


$\Big(j, \nu_p(a_j(x))\Big)$

Montes algorithm (GMN 2009–2012)

Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.
2) For each irreducible factor f_i, write
$f(x) = a_0(x) + a_1(x)f_i(x) + a_2(x)f_i(x)^2 + \cdots + a_g(x)f_i(x)^g$.
3) Determine the f_i-polygon of f,

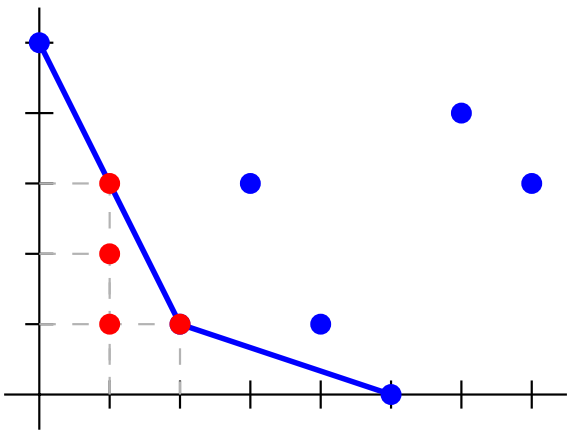


$\Big(j, \nu_p(a_j(x))\Big)$

Montes algorithm (GMN 2009–2012)

Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.
2) For each irreducible factor f_i, write
   $f(x) = a_0(x) + a_1(x)f_i(x) + a_2(x)f_i(x)^2 + \cdots + a_g(x)f_i(x)^g$.
3) Determine the f_i-polygon of f, and compute
   $\mathrm{ind}_{f_i}(f) := \#\{\text{integral points under the polygon}\} \cdot \deg(f_i)$.



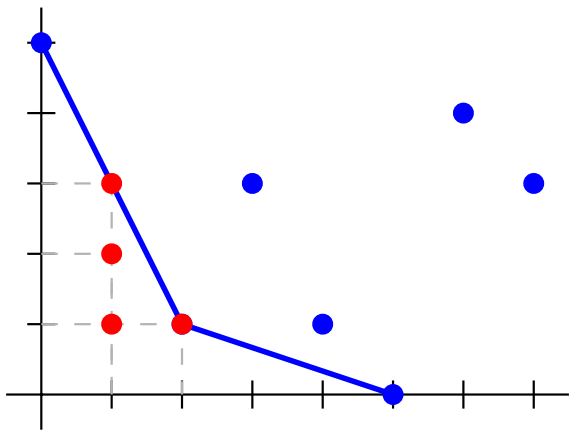
$\big(j, \nu_p(a_j(x))\big)$

$\mathrm{ind}_{f_i}(f) = 4\deg(f_i)$

Montes algorithm (GMN 2009–2012)

Procedure to determine $\mathrm{ind}_p(f)$:

1) Write $f(x) \equiv f_1(x)^{e_1} \cdots f_r(x)^{e_r} \pmod{p}$.
2) For each irreducible factor f_i, write
   $f(x) = a_0(x) + a_1(x)f_i(x) + a_2(x)f_i(x)^2 + \cdots + a_g(x)f_i(x)^g$.
3) Determine the f_i-polygon of f, and compute
   $\mathrm{ind}_{f_i}(f) := \#\{\text{integral points under the polygon}\} \cdot \deg(f_i)$.



$\big(j, \nu_p(a_j(x))\big)$

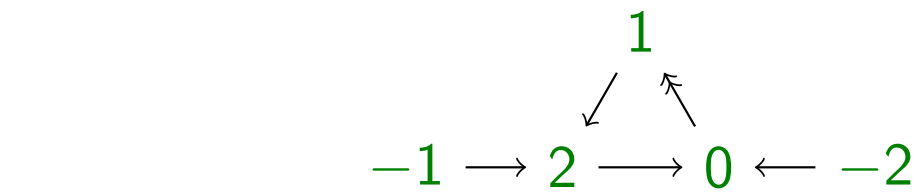
$\mathrm{ind}_{f_i}(f) = 4 \deg(f_i)$

Theorem (Guàrdia–Montes–Nart, 2011)

$\mathrm{ind}_p(f) \geq \sum \mathrm{ind}_{f_i}(f)$ *with equality if* f *is* p*-regular.*

Sketch of proof

$x^2 + 1$ over $\mathbb{F}_5$



Suppose 0 has period m modulo $p > 2$. Then

$$\begin{aligned}
\varphi(x) &\equiv x^2 g_1(x) \pmod{p} \\
\varphi^2(x) &\equiv x^4 g_1(x)^2 g_2(x) \pmod{p} \\
\varphi^3(x) &\equiv x^8 g_x(x)^4 g_2(x)^2 g_3(x) \pmod{p} \\
&\vdots \\
\varphi^n(x) &\equiv \prod_{i=0}^{n} g_i(x)^{2^{n-i}} \pmod{p}, \quad \text{where } g_0(x) = x.
\end{aligned}$$

Sketch of proof

$$\varphi(x) \equiv x^2 g_1(x) \pmod{p}$$

Let ϕ be an irreducible factor of g_1.

ϕ-development of $\varphi(x)$: $\varphi(x) = a_0 + a_1\phi(x) + a_2\phi(x)^2 + \cdots$.

Using Hensel lifting, $\nu_p(a_0) \geq k$, and $\nu_p(a_1) = 0$.

This choice guarantees that the ϕ-polygon associated with φ^n is one-sided.

Sketch of proof

$$\varphi(x) \equiv x^2 g_1(x) \pmod{p}$$

Let ϕ be an irreducible factor of g_1.

ϕ-development of $\varphi(x)$: $\varphi(x) = a_0 + a_1\phi(x) + a_2\phi(x)^2 + \cdots$.

Using Hensel lifting, $\nu_p(a_0) \geq k$, and $\nu_p(a_1) = 0$.

This choice guarantees that the ϕ-polygon associated with φ^n is one-sided.

Obtain the ϕ-development of $\varphi^2(x)$ by composing with f:

$$\varphi^2(x) = f^m \circ \varphi(x) = a_0' + a_1'\phi(x) + a_2'\phi(x)^2 + \cdots .$$

Tracking p-valuations: $\nu_p(a_0') = k, \nu_p(a_1') \geq k$, and $\nu_p(a_2') = 0$.

Sketch of proof

$$\begin{aligned}\varphi^2(x) &= a'_0 + a'_1\phi(x) + a'_2\phi(x)^2 + \cdots \\ &= p^k a''_0 + p^k a''_1\phi(x) + a'_2\phi(x)^2 + \cdots\end{aligned}$$

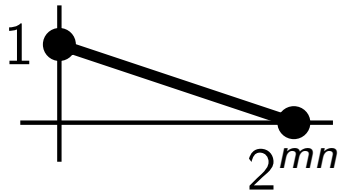
Replace a''_0 and a'_1 with their ϕ-developments to obtain the ϕ-development of φ^2.

In general, the polygon is one a single edge joining $(0, k)$ and $(2^j, 0)$, and we are left to count lattice points.

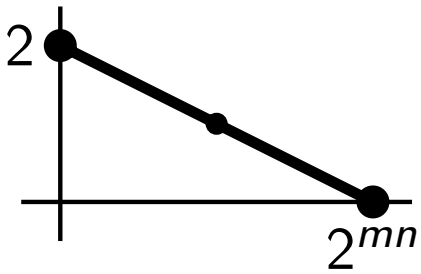
$p = 2$?

For $p = 2$, $\varphi^n(x) \equiv x^{2^{mn}} \pmod 2$, so it is sufficient to consider the usual Newton polygon of φ^n

If $\nu_2(\varphi(0)) = 1$, then the Newton polygon is:



If $\nu_2(\varphi(0)) = 2$, then the Newton polygon of $\varphi(x)$ is:



The residual polynomial associated to this side is $x^2 + 1$, which is not separable over $\mathbb{F}_2$.

Data for f^2:

$c \pmod{32}$	x^2-2	x^2-2x-2	x^2-2x-6
4	[6,6,4]	[8,7,4]	[9,7,4]
12	[8,6,4]	[6,7,4]	[6,7,4]
20	[6,6,4]	[10+,7,4]	[8,7,4]
28	[10+,6,4]	[6,7,4]	[6,7,4]

Data for f^3:

$c \pmod{32}$	x^4-2	x^4-2x^2-2	x^4-2x^2-4x-6
4	[12,12,8]	[16,14,8]	[19,14,8]
12	[16,12,8]	[12,14,8]	[12,14,8]
20	[12,12,8]	[20+,14,8]	[16,14,8]
28	[20+,12,8]	[12,14,8]	[12,14,8]

Data for f^4:

$c \pmod{32}$	x^8-2	x^8-2x^4-2	$x^8-2x^4-4x^3-4x^2-6$
4	[24,24,16]	[32,28,16]	[39,28,16]
12	[32,24,16]	[24,28,16]	
20	[24,24,16]	[40+,28,16]	
28	[40+24,16]	[24,28,16]	

Questions:

- Root discriminant: What are the admissible polygons? Can the 2-adic valuation of the index be bounded?
- Monogenic fields: square-free critical orbits?

Thank you