

The Splitting of Primes in  
 $K(x)[Y]/(Y^3 - AY + B)$

Eric Landquist (UIUC)

and

Jonathan Webster (UIUC)

Joint work with:

Pieter Rozenhart (U Calgary)

Renate Scheidler (U Calgary)

Qingquan Wu (UIUC)

October 28, 2006

# Overview

- \* Motivation
- \* Background - Comparison to Number Fields
- \* Our Result - All Four Cases
- \* Examples of the Proof (Not all four cases.)
- \* Open Question
- \* Questions?

## Motivation

- \* Finding settings suitable for Cryptography.
- \* Don't put all your eggs in one basket.
- \* One need for Crypto: a (sub)group with large prime order, and an efficient way to find it.
- \* Specifically we wish to find an efficient algorithm to find the order of the Jacobian of a cubic function field,  $K$ , over  $\mathbb{F}_q$ .
- \* One method requires approximating the  $L$ -polynomial of  $K$ .
- \* This in turn requires knowledge of the splitting behavior of primes.

## Background

- \* Function fields behave like number fields.
- \* Cubic number field:  $\mathbb{Q}[x]/(f(x))$ , where  $f$  is irreducible and cubic.
- \* Cubic function field:  $\mathbb{F}_q(x)[Y]/(Y^3 - AY + B)$ , where  $A, B \in \mathbb{F}_q[x]$ .
- \* Both have an associated ring of integers.
- \* In number fields, a prime, say (5), may not be prime in an extension,  $\mathbb{Q}[x]/(f(x))$ , of  $\mathbb{Q}$ .
- \* How (5) splits into primes is largely determined by how  $f(x)$  factors mod 5.
- \* In the function field case, primes in  $\mathbb{F}_q(x)$  are irreducible polynomials in  $\mathbb{F}_q[x]$ .
- \* Splitting behavior of a prime  $\mathfrak{p}$  is mostly determined by how  $Y^3 - AY + B$  factors mod  $\mathfrak{p}$ .

## Our Result - Cases I and II

**Case I.**  $p|A$  and  $p|B$

- If  $1 \leq v_p(B) \leq v_p(A)$  then  $p = P^3$ .
- If  $1 = v_p(A) < v_p(B)$  then  $p = PQ^2$ .

**Case II.**  $p \nmid A$  and  $p|B$

In this case  $f(Y) \equiv Y(Y^2 - A) \pmod{p}$

- If  $\left(\frac{A}{p}\right) = 1$  then  $p = PQR$ .
- If  $\left(\frac{A}{p}\right) = -1$  then  $p = PQ$ .

## Our Result - Case III

**Case III.**  $p|A$  and  $p \nmid B$

In this case,  $f(Y) \equiv Y^3 + B \pmod{p}$ .

$\left(\frac{B}{p}\right)_3$  denotes cubic reciprocity. It equals 1 if  $B$  is a cube in the finite field  $\mathbb{F}_{q^{\deg p}}$ .

- $\left(\frac{B}{p}\right)_3 = 1$ 
  - If  $q^{\deg(p)} \equiv 1 \pmod{3}$  then  $p = PQR$ .
  - If  $q^{\deg(p)} \equiv 2 \pmod{3}$  then  $p = PQ$ .
- If  $\left(\frac{B}{p}\right)_3 \neq 1$  then  $p = P$ .

## Our Result - Case IV

### Case IV. $p \nmid AB$

- If  $v_p(\Delta) > 0$  then  $p = PQ^2$ .
- $v_p(\Delta) = 0$ 
  - $v_p(D) = 0$
  - \*  $\left(\frac{-3D}{p}\right) = -1$
  - $\left(\frac{\delta_+^3}{q^{2 \deg p}}\right)_3 = 1$ 
    - i. If  $q^{\deg p} \equiv 1 \pmod{3}$  then  $p = PQ$ .
    - ii. If  $q^{\deg p} \equiv 2 \pmod{3}$   
then  $p = PQR$ .
  - If  $\left(\frac{\delta_+^3}{q^{2 \deg p}}\right)_3 \neq 1$  then  $p = P$ .

$$* \left( \frac{-3D}{p} \right) = 1$$

· If  $q^{\deg(p)} \equiv 2 \pmod{3}$  then  $p = PQ$ .

·  $q^{\deg(p)} \equiv 1 \pmod{3}$

i. If  $\left( \frac{\delta^3}{p} \right)_3 = 1$  then  $p = PQR$ .

ii. If  $\left( \frac{\delta^3}{p} \right)_3 \neq 1$  then  $p = P$ .

–  $v_p(D) > 0$ . That is,  $v_p(D)$  is even.

\* If  $q^{\deg p} \equiv 2 \pmod{3}$  then  $p = PQR$ .

\*  $q^{\deg p} \equiv 1 \pmod{3}$

· If  $\left( \frac{-4B}{p} \right)_3 = 1$  then  $p = PQR$ .

·  $\left( \frac{-4B}{p} \right)_3 \neq 1$  then  $p = PQR$ .

This completes the statement of the result.

## Idea of the Proof

For most cases, we use a result of Dedekind.

**Lemma:** If  $p \nmid I$ , then  $(p)$  factors in  $K$  as  $f(y)$  factors mod  $p$ .

In cases where  $p|I$ , we needed other results. Here are a couple examples of the Lemma in action.

**Case II.**  $p \nmid A$  and  $p|B$ .

In this case  $f(Y) \equiv Y^3 - AY = Y(Y^2 - A)$ .

If  $A$  is a quadratic residue mod  $p$ , then  $(Y^2 - A)$  factors, otherwise it doesn't. So if  $\left(\frac{A}{p}\right) = 1$  then  $p = PQR$ , otherwise if  $\left(\frac{A}{p}\right) = -1$  then  $p = PQ$ .

Note:  $\left(\frac{A}{p}\right) = A^{(|p|-1)/2}$ , where  $|p| = q^{\deg p}$ .

## Idea of the Proof

**Case IV.**  $p \nmid AB$ .

For most of the subcases here, we relied upon finding what extension of  $\mathbb{F}_q$  the roots of the polynomial  $f(Y) = Y^3 - AY + B$  live in.

By Cardano's Formula we have

$$f(Y) = (Y - y_1)(Y - y_2)(Y - y_3) \pmod{p},$$

where

$$y_i = \frac{1}{3} \left( u^i \delta_+ + u^{-i} \delta_- \right), i = 1, 2, 3$$

$u$  is a primitive cube root of unity, and

$$\delta_{\pm} = \sqrt[3]{-\frac{3}{2} \left( 9B \pm \sqrt{-3D} \right)}.$$

## Example of the Proof

Case IV.  $v_p(\Delta) = 0, v_p(D) > 0$ , so  $p|I$ .

$$\gcd(f(Y), f'(Y)) = Y + \frac{3B}{2A}, \text{ so}$$
$$f(Y) = (Y - y_0)^2(Y - y_1) \pmod{p}.$$

Since  $p$  cannot ramify in this case,  $p = PQ$   
or  $p = PQR$ .

$y_0 \in \mathbb{F}_q$ , so where do the other roots live?

$$\delta_{\pm} \equiv \frac{3}{2} \sqrt[3]{-4B}, \text{ so } y_1, y_2 \in \mathbb{F}_{q^{3 \deg p}}.$$

However,  $y_1$  and  $y_2$  are roots of  $Y^2 + y_0Y + (y_0^2 - A)$ , so  $y_1, y_2 \in \mathbb{F}_{q^{2 \deg p}}$ .

They are in a quadratic and cubic extension of  $\mathbb{F}_{q^{\deg p}}$  simultaneously, so they are in  $\mathbb{F}_{q^{\deg p}}$ . Thus  $p$  splits completely.

## Open Question

In Case IV,  $v_p(\Delta) = 0$ ,  $v_p(D) = 0$ ,  
 $\left(\frac{-3D}{p}\right) = -1$ :

We conjecture that if ( $\deg p$  is odd and)  
 $q^{\deg p} \equiv 1 \pmod{3}$ , then  $\left(\frac{\delta_+^3}{q^{2 \deg p}}\right)_3 = 1$ , so  
 $p = PQ$ .

In other words, in the case that  $p \nmid AB$ ,  $v_p(\Delta) = 0$ ,  $v_p(D) = 0$ ,  $\left(\frac{-3D}{p}\right) = -1$ , and  $\left(\frac{\delta_+^3}{q^{2 \deg p}}\right)_3 \neq 1$ , where  $p = P$ , we could have two subcases:

- i) ( $\deg p$  is odd and)  $q^{\deg p} \equiv 1 \pmod{3}$
- ii)  $q^{\deg p} \equiv 2 \pmod{3}$

We conjecture that subcase i) does not occur. If the degree of  $p$  is even in this case, then  $p = PQR$ . This would be picked up under the subcase  $\left(\frac{-3D}{p}\right) = 1$ .