MAXIMAL QUARTICS OVER $\mathbb{F}_{p^2}$

JAAP TOP

A result of Ibukiyama [3] implies that for every odd prime number p, a curve C of genus 3 defined over $\mathbb{F}_{p^2}$ exists which is maximal over $\mathbb{F}_{p^2}$. This means that the number of rational points over $\mathbb{F}_{p^2}$ on the curve satisfies

$$\#C(\mathbb{F}_{p^2}) = p^2 + 1 + 6p.$$

Ibukiyama's proof is not constructive. There are several examples of maximal genus 3 curves (we will recall some here), but a general convenient method that for given p prime constructs one such curve over $\mathbb{F}_{p^2}$ seems unknown.

Here are some examples; see [4]. The Dyck-Fermat curve given by $x^4 + y^4 + z^4 = 0$ is maximal over $\mathbb{F}_{p^2}$, for every prime number $p \equiv 3 \bmod 4$.

The hyperelliptic curve corresponding to $y^2 = x^7 + 1$ is maximal over $\mathbb{F}_{p^2}$, for every prime number $p \equiv 6 \bmod 7$.

The hyperelliptic curve corresponding to $y^2 = (x-2)(x^2-2)(x^4 - 4x^2 + 1)$ is maximal over $\mathbb{F}_{p^2}$, for every prime number $p \equiv 13 \bmod 24$.

Since the Dyck-Fermat curve yields an example over $\mathbb{F}_{p^2}$ for all primes $p \equiv 3 \bmod 4$, it seems natural to supplement this with examples which work for primes $p \equiv 1 \bmod 4$.

Suppose p is an odd prime number. Take λ in an extension field of $\mathbb{F}_p$ such that the elliptic curve E_λ given by $y^2 = x(x-1)(x-\lambda)$ is supersingular. It is known (see, e.g., [1, Prop. 2.2]) that this condition implies that $\lambda \in \mathbb{F}_{p^2}$. Furthermore, by [5, Thm. V-4.1] E_λ is supersingular if and only if

$$H_p(\lambda) := \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i = 0,$$

in which $m = (p-1)/2$. In particular, the polynomial $H_p(x) \in \mathbb{F}_p[x]$ factors as a product of polynomials of degree at most 2.

Now suppose $p \equiv 1 \bmod 4$. Then $H_p(x)$ has no zeroes in $\mathbb{F}_p$, since if λ were such a zero, then $\#E_\lambda(\mathbb{F}_p) = p + 1 \equiv 2 \bmod 4$, contradicting the fact that $E_\lambda(\mathbb{F}_p)$ contains a subgroup of order 4 generated by $(0,0)$ and $(1,0)$.

So if $p \equiv 1 \bmod 4$ then $H_p(x)$ has $(p-1)/4$ pairs of zeroes $\lambda, \lambda^p \in \mathbb{F}_{p^2}$. For any such zero, consider the quadratic twist of E_λ defined as

$$E'_\lambda \ : \ (\lambda+3)y^2 = x(x-1)(x-\lambda).$$

We know from [1, Prop. 2.2] (see also [2,]) that $\#E_\lambda(\mathbb{F}_{p^2}) = p^2+1-2p$. Hence if $\lambda+3$ is not a square in $\mathbb{F}_{p^2}$, then $\#E'_\lambda(\mathbb{F}_{p^2}) = p^2+1+2p$.

In this case, consider the genus 3 curve C_λ over $\mathbb{F}_{p^2}$ given by

$$x^4+y^4+z^4 = (\lambda+1)(x^2y^2+y^2z^2+z^2x^2).$$

From [2, Coroll. 12] we deduce $\#C_\lambda(\mathbb{F}_{p^2}) = p^2+1+6p$. So indeed this yields an explicit maximal curve of genus 3 over $\mathbb{F}_{p^2}$, provided a zero λ of $H_p(x)$ exists such that $\lambda+3$ is not a square. This condition is equivalent to $H_p(x^2-3)$ having an irreducible factor of degree 4 in $\mathbb{F}_p[x]$ (namely, if μ is a zero of such a factor, then $\lambda := \mu^2-3 \in \mathbb{F}_{p^2}$ is a zero of $H_p(x)$ as desired).

In the following table, such a factor is given for each prime $p \equiv 1 \bmod 4$ with $p < 50$. Given the factor x^4+ax^2+b, the corresponding λ is any root of $x^2+(a+6)x+3a+b+9=0$.

5	x^4+3x^2+3
13	x^4+x^2+2
17	x^4+10x^2+11
29	x^4+7x^2+15
37	x^4+17
41	x^4+2x^2+27

Whether or not this method provides a maximal curve over $\mathbb{F}_{p^2}$ for every prime p, I do not know. It works for all $p < 1000$, and the number of factors of degree 4 of $H_p(x^2-3)$ seems to be increasing. So I guess that indeed the method will work for all p.

References

[1] R. Auer and J. Top, *Legendre Elliptic Curves over Finite Fields,* Journal of Number Theory **95** (2002), 303–312.

[2] R. Auer and J. Top, *Some genus 3 curves with many points,* p. 163-171 in *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. **2369**, Springer-Verlag, Berlin, 2002.

[3] T. Ibukiyama, *On rational points on curves of genus 3 over finite fields,* Tôhoku Math. J. **45** (1993), 311–329.

[4] T. Kodama, J. Top, and T. Washio, *Maximal hyperelliptic curves of genus three,* Finite Fields and their Appl. **15** (2009), 392–403.

[5] J.H. Silverman, The Arithmetic of Elliptic Curves. Springer-Verlag, Berlin, 1986.