2013

Pointless Hyperelliptic Curves

Ryan P. Becker
Gettysburg College

Darren B. Glass
Gettysburg College

Becker, Ryan and Darren Glass. "Pointless Hyperelliptic Curves." Finite Fields and Their Applications 21 (2013): 50-57.

Pointless Hyperelliptic Curves

Abstract
In this paper we consider the question of whether there exists a hyperelliptic curve of genus g which is defined over but has no rational points over for various pairs . As an example of such a result, we show that if p is a prime such that is also prime then there will be pointless hyperelliptic curves over of every genus.

Keywords
cryptography, coding theory, hyperelliptic curve

Disciplines
Geometry and Topology | Mathematics | Number Theory

Comments
Ryan P. Becker: Class of 2013

POINTLESS HYPERELLIPTIC CURVES

Ryan Becker
Department of Mathematics, Colorado State University
becker@math.colostate.edu

Darren B Glass
Department of Mathematics, Gettysburg College, Gettysburg PA 17325
dglass@gettysburg.edu

Abstract

In this paper we consider the question of whether there exists a hyperelliptic curve of genus g which is defined over $\mathbb{F}_q$ but has no rational points over $\mathbb{F}_q$ for various pairs (g,q). As an example of such a result, we show that if p is a prime such that $q = \frac{p-1}{2}$ is also prime then there will be pointless hyperelliptic curves over $\mathbb{F}_p$ of every genus $g \geq q-1$.

1 Introduction and Background

The question of constructing curves of a given genus with a given number of points over a finite field is one that many mathematicians have worked on. Because of applications in coding theory, most of the energy has been spent trying to find curves of a fixed genus with as many points as possible – much of this work is described at the website `http://www.manYPoints.org` [13], maintained by Gerard van der Geer and others. Interested readers may wish to consult [1], [2], [4], [6], [7], [8], and [11] among other papers. While it may lack immediate applications, it is nonetheless an interesting mathematical question to consider how few points a curve of a given genus might have, and in particular whether there exist curves of a given genus that do not have any points defined over a fixed finite field. For small genera, this question was considered in [5] and [9], where the authors proved the following results.

Theorem 1.1. *The following conditions on the existence of pointless curves are both necessary and sufficient:*

- *There exist pointless curves of genus* 2 *defined over* $\mathbb{F}_q$ *if and only if* $q < 13$.
- *There exist pointless curves of genus* 3 *defined over* $\mathbb{F}_q$ *if and only if* $q \leq 25, q = 29$ *or* $q = 32$.
- *There exist pointless hyperelliptic curves of genus* 3 *defined over* $\mathbb{F}_q$ *if and only if* $q \leq 25$.
- *There exist pointless curves of genus* 4 *defined over* $\mathbb{F}_q$ *if and only if* $q \leq 49$.

The results of Theorem 1.1 fix a genus and let the field vary; in this note, we take the complementary point of view and fix our finite field and consider for which genera there exists a pointless curve. A recent result of Stichtenoth in [10] proved that for each finite field $\mathbb{F}_q$, there exists a number g_q so that for all $g \geq g_q$ there is a pointless curve over $\mathbb{F}_q$ of genus g. In this note, we consider the analogous question for hyperelliptic curves. In particular, Section 2 gives two types of explicit constructions of pointless hyperelliptic curves of various genera which give bounds on g_q. One of these relies on the value of g mod q and the other on the value of g mod $q-1$. Examples of such results are:

Theorem 1.2. *Let a be the least residue of g mod p so that $a < p-1$. There exists a $2p+2$-pointed curve of genus g defined over $\mathbb{F}_q$ if $g \geq (p-a-1)(q-1)$. If $0 \leq a \leq \frac{p-3}{2}$, then there exists a $2p+2$-pointed curve of genus g if $g \geq \frac{q-1}{2}(p-2a-2)$.*

Theorem 1.3. *Let $(g+1, \frac{p-1}{2}) = 1$ and $g \geq \frac{p-3}{2}$. Then there is a pointless hyperelliptic curve of genus g over $\mathbb{F}_p$.*

In particular, we note that if p is a prime such that $q = \frac{p-1}{2}$ is also prime (ie q is a Sophie Germain prime) then there will be pointless hyperelliptic curves over $\mathbb{F}_p$ of every genus $g \geq q-1$.

In Section 3, we combine these results as well as some results about fibre products of hyperelliptic curves to give explicit numerical bounds for when pointless hyperelliptic curves can exist over a specific finite field. These results show that in general there is a linear bound on q above which one can obtain all genera. We note that Serre's bound says that there is a lower bound on the order of $\sqrt{q}$ below which we cannot obtain any pointless hyperelliptic curves. In future work, we hope to explore the gap between these two bounds.

2 Existence Results

Before we prove our main results, we begin by introducing some notation. Let $\mathbb{F}_q$ be the field of odd order $q = p^r$ and let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ by the equation $y^2 = f(x)$. Let n be the number of points of C defined over $\mathbb{F}_q$. If we choose $a \in \mathbb{F}_q$ to be a nonsquare and define $\tilde{C}$ to be the quadratic twist of C given by $y^2 = af(x)$, then $\tilde{C}$ will be a hyperelliptic curve of genus g with $2q+2-n$ points defined over $\mathbb{F}_q$. In particular, there will be pointless hyperelliptic curves over $\mathbb{F}_q$ if and only if there are curves with $2q+2$ points over $\mathbb{F}_q$. It is often convenient to consider these curves, which have the maximal number of points allowable for hyperelliptic curves, instead of curves with no points.

As an example of this approach, let $p \geq 7$ and consider the curve C_g defined by the equation $y^2 = f(x) = x^{q-1} + \alpha$ where $\alpha \in \mathbb{F}_p$ is a quadratic residue such that $\alpha+1$ is also a quadratic residue. We note that such an α must exist as at least one of the set $\{2,5,10\}$ must be a residue. This curve is nonsingular, as $f'(x)$ only has roots at $x = 0$ and $f(0) \neq 0$. Therefore, it is a hyperelliptic curve of genus $g = \frac{q-3}{2}$. Moreover, $f(0) = \alpha$ is a residue and for all $x \in \mathbb{F}_q^*$ we have that $f(x) = \alpha + 1$ is also a residue so there are two points lying over each $x \in \mathbb{F}_q$. Finally, because $f(x)$ is monic of even degree there are two points lying over infinity and therefore C_g has $2q+2$ points. This implies that $\tilde{C_g}$ is a pointless hyperelliptic curve of genus g, proving the following lemma.

Lemma 2.1. *Let $p \geq 7$. Then there exist pointless hyperelliptic curves of genus $g = \frac{q-3}{2}$ defined over $\mathbb{F}_q$.*

Throughout this section, we will construct monic polynomials $f(x)$ of various degrees n which have no repeated roots and such that $f(x)$ is a quadratic residue for all $x \in \mathbb{F}_q$. As in the above discussion, $y^2 = f(x)$ will then define a nonsingular hyperelliptic curve of genus $g = \frac{n-2}{2}$ over $\mathbb{F}_q$ with $2q+2$ points, and a quadratic twist by a nonresidue will therefore be a pointless hyperelliptic curve of the same genus. We note that our constructions all take advantage of the fact that for all $x \in \mathbb{F}_q^*$ we have that $x^{q-1} = 1$, and in particular we will only construct polynomials of degree $n \geq q-1$. Therefore, we never construct curves of genus $g < \frac{q-3}{2}$.

Lemma 2.2. *Assume that $g \equiv -1$ (mod p) and $g > \frac{q-3}{2}$. Then there exist pointless hyperelliptic curves of genus g defined over $\mathbb{F}_q$.*

Proof. Consider the curve C_g defined by the equation

$$y^2 = f(x) = x^{2g+2} - x^{2g+2-q+1} + 1$$

where $2g+2 \geq q$. It is clear that for any $x \in \mathbb{F}_q$, $f(x) = 1$ and therefore there will be two points lying over each x value. Moreover, $f(x)$ is monic of even degree, so there are also two points lying over $x = \infty$. It follows that C_g has $2q+2$ points over $\mathbb{F}_q$ and that the quadratic twist $\tilde{C_g}$ is pointless. In order to show that the curves C_g and $\tilde{C_g}$ have genus g, it suffices to show that they are nonsingular. In particular, we wish to show that $f(x)$ has no repeated roots over $\overline{\mathbb{F}_q}$. It follows from our hypothesis that $p|2g+2$ and therefore that $f'(x) = (q-1)x^{2g+2-q}$ will have no roots in common with $f(x)$. □

A variation on this approach will work more generally, allowing us to give the following proof of Theorem 1.2.

Proof. For $0 \leq a \leq p-2$ and $g \geq (p-a-1)(q-1)$, set $l = -(2a+2)+2p$. In particular, we note that $l \equiv -(2a+2) \equiv -(2g+2) \bmod p$. Moreover, a simple calculation shows that $2g+2 > l(q-1) > 0$. As in the discussion proving Lemma 2.2, we consider the equation $f(x) = x^{2g+2} - x^{2g+2-l(q-1)} + 1$. It is a straightforward computation to see that $f'(x) = (2g+2)x^{2g+1}$ and therefore that all roots of $f'(x)$ are 0. However, $f(0) \neq 0$, so $f(x)$ and $f'(x)$ do not share any roots. This implies that the curve defined by $y^2 = f(x)$ is a nonsingular hyperelliptic curve of genus g. Moreover, for each $x \in \mathbb{F}_q$ it is clear that $f(x) = 1$ and therefore there are two choices of y which correspond to this x, and the fact that $f(x)$ is monic implies that there are two points over ∞. Thus, the curve has $2q+2$ points.

If $a \leq \frac{p-3}{2}$, then we can improve the bound on g by instead setting $l = -(2a+2)+p$. This choice of l will satisfy the requirements that $l \equiv -(2g+2) \bmod p$ and $2g+2 > l(q-1) > 0$ as long as $g \geq \frac{q-1}{2}(p-2a-2)$. This proves the stated theorem. □

In the case where we are working over a prime field, the above result simplifies to the following:

Corollary 2.3. *Let a be the least residue of g mod p. Then there exist pointless hyperelliptic curves of genus g over $\mathbb{F}_p$ if $g \geq (p-a)(p-2)$. In particular, there will be pointless hyperelliptic curves of every genus $g \geq \frac{(p+1)(p-2)}{2}$.*

We get a different type of result by considering the congruence class of g mod $q-1$ rather than mod q. In order to do this, let us prove the following theorem:

Theorem 2.4. *Let p be a prime number, q be a power of p, and $n \geq q$. Define d to be $gcd(n, q-1)$ and assume that $n^d \not\equiv (n+1)^d \bmod p$. Then the equation $f(x) = x^n - x^{n-(q-1)} + 1$ has no multiple roots.*

Proof. If $n \equiv 0$ or $-1 \bmod p$ then $f'(x)$ is seen to be a power of x and therefore has no roots in common with $f(x)$, proving the claim.

For the remaining cases, we proceed by contradiction and assume that $\gamma \in \overline{\mathbb{F}_p}$ is a double root of $f(x)$, so in particular $f(\gamma) = f'(\gamma) = 0$. Then $f'(\gamma) = n\gamma^{n-1} - (n-q+1)\gamma^{n-q} = 0$. In particular, we have that $n\gamma^{n-1} = (n-q+1)\gamma^{n-q}$. Note that $\gamma = 0$ is not a root of $f(x)$, so we must have $\gamma^{q-1} = \frac{n-q+1}{n}$.

To proceed, we write $n = k(q-1)+j$ with $0 \leq j < q-1$. Using the fact that $\gamma^{q-1} = \frac{n-q+1}{n}$, we compute

$$0 = f(\gamma) = \left(\frac{n-q+1}{n}\right)^k \gamma^j - \left(\frac{n-q+1}{n}\right)^{k-1} \gamma^j + 1$$

This allows us to deduce that $\gamma^j \in \mathbb{F}_q$, so that $(\gamma^{q-1})^j = (\gamma^j)^{q-1} = 1$. Noting that $gcd(j, q-1) = gcd(n, q-1) = d$ and that $(\gamma^{q-1})^j = (\gamma^{q-1})^{q-1} = 1$, it follows that $(\gamma^{q-1})^d = 1$. This implies that $\left(\frac{n-q+1}{n}\right)^d = 1$, or that $n^d \equiv (n+1)^d \bmod p$, giving us a contradiction. The lemma is an immediate consequence. □

Looking at the quadratic twist of the curve defined by the equation $y^2 = x^n - x^{n-(q-1)} + 1$, the following result is an immediate corollary:

Corollary 2.5. *For a given $g \geq \frac{q-1}{2}$, set $d = gcd(2g+2, q-1)$. If $(2g+2)^d \not\equiv (2g+3)^d \pmod p$ then there exists a pointless hyperelliptic curve of genus g defined over $\mathbb{F}_q$.*

Example 2.6. As an example of Corollary 2.5, we consider curves over $\mathbb{F}_q$ of genus $g = q-4$. In this case, $2g+2 = 2q-6$, so $d = gcd(2g+2, q-1) = gcd(q-1, 4)$ will be equal to 4 (resp. $d = 2$) if $q \equiv 1$ (resp. $q \equiv 3$) (mod 4). In particular, Corollary 2.5 implies that the curve defined by $y^2 = x^{2q-6} - x^{q-5} + 1$ will be nonsingular except possibly in cases where $5^4 = 6^4$. This implies the existence of a pointless hyperelliptic curve of genus $q-4$ unless $p = 11$ or $p = 61$. We note that there does exist a pointless hyperelliptic curve of genus 7 over $\mathbb{F}_{11}$ as will follow from Theorem 1.3.

A similar argument will show that there exist pointless hyperelliptic curves defined over $\mathbb{F}_q$ of genus $g = q-a$ as long as $g \geq \frac{q-1}{2}$ and $p \not| ((2a-2)^{2a-4} - (2a-3)^{2a-4})$. This gives an explicitly computable finite

set of characteristics away from which we will have pointless hyperelliptic curves of a given genus. This approach generalizes, and while stating a result in full generality is difficult, we give one example below of such a result over $\mathbb{F}_p$. Note that $2g+2$ and $p-1$ are both even, so at best we have that $(2g+2, p-1) = 2$, which is equivalent to the condition that $g+1$ and $\frac{p-1}{2}$ are relatively prime. For notational convenience, we set $p' = \frac{p-1}{2}$.

Theorem 2.7. *Let p be an odd prime and $n \geq p$ an integer with $gcd(n, p-1) = 2$. Then the equation $x^n - x^{n-p+1} + 1$ has repeated roots over $\overline{\mathbb{F}_p}$ if and only if one of the following cases hold:*

- *$p \equiv 3$ mod 8 and $n \equiv 0$ (mod 4)*
- *$p \equiv 5, 7$ mod 8 and $n \equiv 2$ (mod 4)*

Proof. Assume that γ is a root of $f(x)$. The proof of Theorem 2.4 implies that γ will have multiplicity greater than one if and only if $(\gamma^{p-1})^2 = \left(\frac{n-p+1}{n}\right)^2 = 1$. In particular, this implies that $\gamma^{p-1} \equiv -1 \bmod p$ which in turn implies that $\gamma^n = p'$. Moreover, the fact that $\gamma^{p-1} \equiv -1$ tells us that $\gamma \notin \mathbb{F}_p$ but that $\alpha = \gamma^2$ is a quadratic nonresidue in $\mathbb{F}_p$. By our hypothesis, n is even and we consider the cases $n \equiv 0$ and $n \equiv 2$ (mod 4) separately. If $n = 4k$ then we see that $\alpha^{2k} \equiv p'$, implying that p' is a quadratic residue mod p which will happen if and only if $p \equiv 1$ or 3 (mod 8). However, if n is a multiple of 4 then p cannot be by hypothesis, so we must have $p \equiv 3$ mod 8. Similarly, if $n = 4k+2$ then $\alpha^{2k+1} \equiv p'$ which implies that p' is a nonresidue, so $p \equiv 5$ or 7 (mod 8).

To see the converse, we first consider the case where $p \equiv 5$ or 7 (mod 8) and $n = 4k+2$. We note that there will be a unique solution to the equation $x^{2k+1} \equiv p' \bmod p$ because $gcd(2k+1, p-1) = 1$. Let us call this solution α and let γ be one of the square roots of α in $\overline{\mathbb{F}_p}$. Because p' is a quadratic nonresidue it must be the case that α is as well. Therefore $\gamma^n = p'$ and $\gamma^{p-1} = -1$ which implies that $f(\gamma) = f'(\gamma) = 0$.

Next we consider the case where $p \equiv 3$ mod 8 and $n = 4k$. In this case, p' is a quadratic residue mod p and there will be two solutions to the equation $x^2 \equiv p'$ (mod p). Because -1 is a nonresidue, exactly one of these solutions will also be a nonresidue, and we choose β to be this solution. Because $gcd(k, p-1) = 1$ there will be a unique choice of $\alpha \in \mathbb{F}_p$ so that $\alpha^k = \beta$. Finally, we can choose γ to be one of the solutions to $x^2 = \alpha$ in $\overline{\mathbb{F}_p}$. It follows that $\gamma^n = p'$. Moreover, because β is a nonresidue it follows that α will be as well so that $\gamma^{p-1} \equiv -1$. Thus, $f(\gamma) = f'(\gamma) = 0$.

In either case, we have constructed an element γ which is a root of $f(x)$ with multiplicity higher than one. The theorem follows. □

We now give a proof of Theorem 1.3.

Proof. Assume that $g \geq p'$ and $g+1$ is relatively prime to p'. Corollary 2.5 implies that there are pointless hyperelliptic curves defined over $\mathbb{F}_p$ except possibly in the case where $(2g+2)^2 \equiv (2g+3)^2 \bmod p$. Clearly $2g+2 \not\equiv 2g+3$, so it suffices to consider the case where $2g+2 \equiv -(2g+3)$. It follows from elementary number theory that we only need to consider the case where $2g+2 \equiv p'$ (mod p).

We now turn to Theorem 1.2, which tells us that if $2g+2 \equiv p' \bmod p$ then we can construct pointless hyperelliptic curves as long as $g > \frac{p^2-5}{4}$.

In particular, the only cases not covered by the theorems above are those genera in the range $[\frac{p-1}{2}, \frac{p^2-5}{4}]$ which are congruent to $\frac{p^2-5}{4} \bmod p$. In each of these cases, the equation $x^{2g+2} - x^{2g+2-(p-1)} + 1$ has repeated roots by Theorem 2.7 but the genus is too small to consider curves of the form $x^{2g+2} - x^{2g+2-\ell(p-1)} + 1$ for $\ell > 1$. □

While the conditions in Corollary 2.5 are sufficient to prove the existence of a pointless hyperelliptic curve of a given genus, they are certainly not necessary, and one can use similar methods to get a different set of sufficient conditions, as one can see in the following theorem.

Theorem 2.8. *Let $n = k(q-1)$ where $k \geq 2, p \not| k$, and $a^2k^k \not\equiv (k-1)^{k-1} \bmod p$ for some $a \in \mathbb{F}_p^*$. Then the equation $f(x) = x^n - x^{n-q+1} + a^2$ has no roots of multiplicity greater than one.*

Proof. Assume that γ is a root of $f(x)$ of multiplicity greater than one. Then $f'(\gamma) = 0$ and a simple computation shows that this implies that either $\gamma = 0$ or $\gamma^{q-1} = \frac{k-1}{k} \in \mathbb{F}_q$. Clearly $f(0) \neq 0$ so we must be in the latter case. We now compute:

$$\begin{aligned} 0 &= f(\gamma) \\ &= \gamma^k(q-1) - \gamma^{k-1}(q-1) + a^2 \\ &= \left(\frac{k-1}{k}\right)^k - \left(\frac{k-1}{k}\right)^{k-1} + a^2 \\ &= \frac{a^2k^k - (k-1)^{k-1}}{k^k} \end{aligned}$$

which implies that $a^2k^k \equiv (k-1)^{k-1} \bmod p$, giving us a contradiction. □

Corollary 2.9. *Let $\mathbb{F}_q$ be a finite field of characteristic $p > 3$. There exist pointless hyperelliptic curves of genus g defined over $\mathbb{F}_q$ if $g \equiv -1$ (mod $\frac{q-1}{2}$) and $g \geq q-2$.*

Proof. The hypothesis imply that $g = \frac{kq-k-2}{2}$ for some $k \geq 2$ so that $2g+2 = k(q-1)$. If k is a multiple of p then $g \equiv -1 \bmod p$, in which case we are covered by Lemma 2.2. For the remainder of this proof, we assume that $p \not| k$.

From Theorem 2.8 it follows that $y^2 = x^{2g+2} - x^{2g+2-q+1} + 1$ is a nonsingular curve of genus g with $2q+2$ points if $2g+2 = k(q-1)$ for some k such that $k^k \not\equiv (k-1)^{k-1} \bmod p$. It also follows that $y^2 = x^{2g+2} - x^{2g+2-q+1} + 4$ is a nonsingular curve with $2q+2$ points as long as $4k^k \not\equiv (k-1)^{k-1} \bmod p$. Therefore, one of these two curves will be nonsingular as long as $4k^k \not\equiv k^k$, which is guaranteed by the hypotheses. Considering a quadratic twist by a nonresidue gives a pointless hyperelliptic curve of genus g as desired. □

3 Numerical Results

In this section, we construct tables of genera unobtainable using the above theorems for all odd primes less than 100. For each prime p, we begin by checking, for all genera less than the bound established by Corollary 2.3, whether the conditions of Theorem 1.2 are satisfied. We thereby obtain a set of genera unobtainable using that result alone. We further prune this set using the conditions of Theorem 2.7 and 1.3, as well as Corollaries 2.5 and 2.9. Another result that will be useful in our computations is the following theorem.

Theorem 3.1. *Let C be a pointless hyperelliptic curve of genus g defined by the equation $y^2 = f(x)$. Then the equation $y^2 = f(x^2)$ defines a pointless hyperelliptic curve of genus $2g+1$.*

One can prove this theorem in several manners. We give a proof involving fibre products as the technique will be useful later on.

Proof. The fact that C has no points defined over $\mathbb{F}_q$ implies in particular that $f(x)$ has degree $2g+2$ and that $f(0) \neq 0$. In particular, neither 0 nor ∞ is a ramification point of $f(x)$. We wish to consider the normalization of the fibre product of C with the hyperelliptic cover given by $z^2 = x$ which is branched only at the points $x = 0, \infty$. It follows from results about fibre products of hyperelliptic curves (see [3], [12] for details and similar constructions) that this curve will have genus $2g+1$ and will have no points defined over $\mathbb{F}_q$. This curve is equivalent to the one defined by $y^2 = f(x^2)$ after a change of variables. □

The table in Figure 1 gives a list of genera that our methods are unable to construct ('missed genera') for $p \leq 100$. As discussed above, our methods can only address those genera which are at least $\frac{p-3}{2}$, so we leave those off of the table. However, this list is otherwise complete.

Note that some of the genera that our methods fail to produce can be produced by other methods such as those in [5]. Moreover, these numerical results do not take into account how $f(x)$ factors over $\mathbb{F}_p$, as these computations are beyond the scope of the program used. However, one can prove the following result.

Theorem 3.2. *Let C be a pointless hyperelliptic curve of genus g defined by the equation $y^2 = f(x)$.*

- *If $f(x)$ has any factor over $\mathbb{F}_p$ that is not given by an irreducible quadratic equation then there exists a pointless hyperelliptic curve of genus $2g$.*
- *If $f(x)$ has a factor defined by an irreducible quadratic equation over $\mathbb{F}_p$ then there exists a pointless hyperelliptic curve of genus $2g-1$.*

The proof of Theorem 3.2 is similar to the proof of Theorem 3.1. However, instead of taking a fibre product with a cover defined by a quadratic equation sharing no roots with $f(x)$ we instead take the fibre product with a cover defined by a quadratic equation which shares either one or two roots with $f(x)$, whose existence is guaranteed by the hypothesis. We omit the details of the proof, but conclude with an example.

Example 3.3. Let C be the nonsingular hyperelliptic curve defined over $\mathbb{F}_{13}$ by the equation $y^2 = f(x) = x^{22} - x^{10} + 1$. The quadratic twist $\tilde{C}$ of this curve by a quadratic nonresidue is a pointless hyperelliptic curve as genus $g = 10$ as discussed in Section 2. Moreover, one can check that over $\mathbb{F}_{13}$ this polynomial has $x^3 + 2x^2 + 7x + 10$ as a factor. Theorem 3.2 now gives us a way of explicitly computing a pointless hyperelliptic curve of genus 20 over $\mathbb{F}_{13}$, eliminating another case from the above table.

Acknolwedgments

We would like to thank the Andrew W. Mellon Foundation and Gettysburg College for their generous support of the first author during this project. We would also like to thank the anonymous referee for several helpful suggestions to improve the content and the exposition of this note.

References

[1] Stefania Fanali and Massimo Giulietti, *On some open problems on maximal curves*, Des. Codes Cryptogr. **56** (2010), no. 2-3, 131–139. MR 2658926 (2011g:11117)

[2] Massimo Giulietti and Gábor Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245. MR 2448446 (2010h:14036)

[3] D. Glass and R. Pries, *On the moduli space of Klein four covers of the projective line*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 58–70. MR MR2181873

[4] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008. MR 2386879 (2008m:14040)

[5] Everett W. Howe, Kristin E. Lauter, and Jaap Top, *Pointless curves of genus three and four*, Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 125–141. MR 2182840 (2006g:11125)

[6] Kristin Lauter, *Improved upper bounds for the number of rational points on algebraic curves over finite fields*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 12, 1181–1185. MR 1701382 (2000e:11079)

[7] Jean-Pierre Serre, *Nombres de points des courbes algébriques sur* $\mathbf{F}_q$, Seminar on number theory, 1982–1983 (Talence, 1982/1983), Univ. Bordeaux I, Talence, 1983, pp. Exp. No. 22, 8. MR 750323 (86d:11051)

[8] ———, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 9, 397–402. MR 703906 (85b:14027)

[9] H. M. Stark, *On the Riemann hypothesis in hyperelliptic function fields*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 285–302. MR 0332793 (48 #11119)

[10] Henning Stichtenoth, *Curves with a prescribed number of rational points*, Finite Fields Appl.

[11] Jaap Top, *Curves of genus 3 over small finite fields*, Indag. Math. (N.S.) **14** (2003), no. 2, 275–283. MR 2027781 (2005g:11113)

[12] G. van der Geer and M. van der Vlugt, *Fibre products of artin-schrier curves and generalized hamming weights of codes*, Journal of Combinatorial Theory, Series A (1995).

[13] Gerard van der Geer, Everett Howe, Kristin Lauter, and Christophe Ritzenthaler, *manypoints table of curves with many points*, `http://www.manYPoints.org`.

p	Missed Genera Greater Than $(p-5)/2$
3	$\emptyset$
5	$\emptyset$
7	$\emptyset$
11	$\emptyset$
13	8, 20
17	$\emptyset$
19	14, 32, 38, 50
23	$\emptyset$
29	48, 62, 118, 132, 146, 174
31	17, 19, 64, 84, 110, 146, 158, 174, 294, 296
37	25, 26, 56, 80, 86, 98, 134, 152, 170, 173, 230, 242, 278, 374, 500
41	34, 44, 54, 94, 189, 214, 334, 374, 394, 454
43	27, 50, 74, 76, 98, 118, 160, 202, 244, 260, 308, 328, 332, 496, 518, 580
47	$\emptyset$
53	31, 64, 116, 142, 168, 194, 220, 272, 298, 428, 454, 532, 636
59	$\emptyset$
61	44, 49, 53, 57, 62, 74, 124, 158, 174, 224, 236, 344, 349, 380, 404, 414, 428, 464, 494, 524, 554, 594, 614, 624, 654, 704, 734, 746, 794, 824, 834, 890, 1074, 1160, 1256, 1344, 1526
67	47, 76, 116, 142, 206, 208, 248, 274, 318, 384, 386, 417, 450, 472, 518, 608, 650, 788, 912, 920, 945, 1010, 1052, 1110, 1412
71	48, 62, 64, 97, 194, 258, 272, 324, 374, 426, 434, 468, 482, 510, 517, 545, 604, 724, 762, 904, 930, 965, 1034, 1042, 1144, 1252, 1314, 1420, 1462, 1744, 2024
73	39, 53, 65, 104, 134, 206, 236, 242, 269, 338, 368, 422, 458, 485, 566, 572, 620, 674, 776, 782, 806, 845, 890, 926, 1106, 1112, 1142, 1214, 1241, 1244, 1652, 1682, 1934, 2120
79	50, 90, 220, 224, 266, 374, 376, 480, 482, 524, 532, 688, 698, 792, 844, 848, 870, 948, 956, 998, 1234, 1322, 1390, 1430, 1472, 1858, 1897, 1904, 1946
83	$\emptyset$
89	47, 57, 67, 76, 98, 208, 230, 340, 384, 582, 681, 692, 714, 769, 934, 1000, 1308, 1385, 1429, 1616, 1660, 1792, 1924, 2056, 2188, 2540, 2672, 2892
97	65, 71, 77, 79, 89, 134, 272, 314, 356, 494, 716, 854, 896, 938, 1076, 1436, 1478, 1520, 1658, 2060, 2102, 2240, 2684, 2822, 3404

Figure 1: Missed Genera For All Primes Less Than 100