

Curves with Many Points over Finite Fields

Gerard van der Geer
Korteweg-de Vries-Instituut
Universiteit van Amsterdam
geer@science.uva.nl
joint with [M. van der Vlugt](#)

November 22, 2005

1801

Let p be a prime. Gauss counted the solutions $f(x, y) = 0 \pmod{p}$ for certain $f(x, y) \in \mathbf{Z}[x, y]$. In §358 of his *Disquisitiones Arithmeticae* he counts the number of solutions of the Fermat curve C

$$x^3 + y^3 + z^3 \equiv 0 \pmod{p}$$

His answer: if $p \equiv 1 \pmod{3}$ write

$$4p = a^2 + 27b^2 \quad \text{with } a \equiv 1 \pmod{3}.$$

Then for $p \neq 3$ the number of solutions is:

$$\#C(\mathbf{F}_p) = \begin{cases} p + 1 & \text{if } p \not\equiv 1 \pmod{3} \\ p + 1 + a & \text{otherwise} \end{cases}$$

Note that then $|a| \leq 2\sqrt{p}$.

During most of this long history nothing happened.

1830: **Galois** invented finite fields \mathbf{F}_q of cardinality $q = p^m$; they are given by $X^{p^m} - X = 0$. But it took till 1893 that **Moore** proved that these are all. Nobody seemed interested in counting points on curves over finite fields till the turn of the century (19/20th).

The *zeta function*, introduced by around 1924 by [Emil Artin](#),

$$Z_C(t) = \exp \left(\sum_{r=1}^{\infty} \#C(\mathbf{F}_{q^r}) \frac{t^r}{r} \right)$$

stores the information about rational points over extension fields and we know after [Hasse](#) ($g = 1$) and [Weil](#) that

$$Z_C(t) = \frac{P(t)}{(1-t)(1-qt)}$$

with

$$P_X(t) = \prod_{i=1}^g (1 - \alpha_i t)(1 - \bar{\alpha}_i t) \in \mathbf{Z}[t]$$

so that

$$Z_C(t) = \frac{\prod_{i=1}^g (1 - \alpha_i t)(1 - \bar{\alpha}_i t)}{(1 - t)(1 - qt)}$$

with algebraic integers α_i satisfying

$$|\alpha_i| = \sqrt{q}.$$

We get the **Hasse-Weil bound**

$$\#X(\mathbf{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r \leq q^r + 1 + 2g\sqrt{q^r}.$$

This upper bound is sharp: the *Hermitian* curve

$$x^{q+1} + y^{q+1} + z^{q+1} = 0$$

has $g = q(q-1)/2$ and $\#C(\mathbf{F}_{q^2}) = q^3 + 1 = q^2 + 1 + 2g\sqrt{q^2}$.

IMPROVED UPPER BOUNDS

Interest was lost again till coding theory brought it back. Ihara had a simple and elegant idea: Note

$$\#X(\mathbf{F}_q) \leq \#X(\mathbf{F}_{q^2});$$

Use $\#X(\mathbf{F}_{q^r}) = q^r + 1 - \sum_{i=1}^r \alpha_i^r$ and apply Cauchy-Schwartz to the g real numbers $\alpha_i + \bar{\alpha}_i$.

Ihara's bound:

$$\#X(\mathbf{F}_q) \leq q + 1 + \left[\sqrt{(8q + 1)g^2 + 4(q^2 - q)g - g} - g \right] / 2$$

which is better than Hasse-Weil if

$$g > (q - \sqrt{q})/2.$$

This was generalized by [Drinfeld-Vladuts](#).

The question arises:

What is the maximum number of rational points on a curve of genus g over a field \mathbf{F}_q ?

For a pair (q, g) we set

$$N_q(g) = \max_X \{ \#X(\mathbf{F}_q) : X/\mathbf{F}_q \text{ and } g(X) = g \}$$

The actual value of $N_q(g)$ for small values of q and g is interesting.

Serre transplanted the ‘**formules explicites**’ of number theory.
Take an even trigonometric polynomial

$$f = 1 + 2 \sum_{n \geq 1} u_n \cos n\theta$$

with $u_n \in \mathbf{R}_{\geq 0}$ such that $f(\theta) \geq 0$ on \mathbf{R} and set

$$\psi = \sum_{n \geq 1} u_n t^n.$$

Then one gets the estimate

$$N_q(g) \leq a_f g + b_f,$$

where

$$a_f = 1/\psi(1/\sqrt{q}), \quad b_f = 1 + \psi(\sqrt{q})/\psi(1/\sqrt{q}).$$

Oesterlé found the optimal f : Oesterlé bounds.

Serre initiated the study of $N_q(g)$. E.g., he determined $N_q(g)$ for $q = 2$ and $1 \leq g \leq 12$.

By Hasse-Weil $N_q(g) \leq q + 1 + [2g\sqrt{q}]$. Serre improved this to

$$N_q(g) \leq q + 1 + g[2\sqrt{q}] .$$

- Upper bounds (Hasse-Weil, Ihara, Serre, Oesterlé, Howe-Lauter)
- Lower bound: best curve we know

How good are these bounds?

We have $N_q(g) \in [a, b]$ with $b =$ best upper bound, $a =$ maximum value we know for $\#C(\mathbf{F}_q)$.

The Table of Wirtz.

$g \backslash q$	2	3	4	8	9	16	27	32	64	81	128
1	5	7	9	14	16	25	38	44	81	100	150
2	6	8	10	18	20	33	48	53	97	118	172
3	7	10	14	24	28	38	55 - 58	62 - 66	113	136	184 - 195
4	8	12	15	-29	26 - 30	41 - 49	55 - 68	65 - 77	129	154	200 - 217
5	9	-15	-18	-32	-36	-57	55 - 78	-88	101 - 145	152 - 172	202 - 239
6	10	-17	17 - 21	25 - 36	29 - 40	65	64 - 88	73 - 99	137 - 161	190	225 - 261
7	10	-19	-23	25 - 39	28 - 43	49 - 70	64 - 98	81 - 110	177	160 - 208	241 - 283
8	11	-21	-25	-43	-47	-76	-108	-121	-193	-226	257 - 305
9	12	-23	-28	33 - 47	37 - 51	49 - 81	82 - 118	81 - 132	173 - 209	244	209 - 327
10	12 - 13	-25	-30	-50	-55	61 - 87	-128	-143	139 - 225	226 - 262	-349
11	13 - 14										
12	14 - 15			37 - 57	37 - 63	61 - 97	91 - 148		257	226 - 298	193 - 393
13	14 - 15								169 - 273	163 - 316	
14	15 - 16			65	43 - 70	81 - 108		113 - 187	193 - 289	218 - 334	289 - 437
15	17			43 - 68		49 - 113		97 - 196	197 - 305		369 - 459
16	16 - 18				46 - 78		100 - 178		199 - 321	370	
17	17 - 18										
18	18 - 19						107 - 192				201 - 525
19	20										
20	19 - 21										
21	21			57 - 89	64 - 97	89 - 145		121 - 244	257 - 401	250 - 460	297 - 591
24					64 - 108		136 - 235		242 - 449	298 - 514	
26								157 - 283			
27											
28				65 - 114	73 - 123	97 - 181	136 - 263	137 - 298	513	313 - 568	409 - 745
30						81 - 192	157 - 277	129 - 313	257 - 536	370 - 586	369 - 789
35						105 - 218					
36					82 - 154		184 - 319			730	
39	33										
42						113 - 254	157 - 360				
45								193 - 428	401 - 706		561 - 1119
48							244 - 402				
49						129 - 291					
50	40										

Around 1995 Van der Vlugt and I started a

Table of Curves with Many Points.

The outcome is distilled from the work of many people. We have various methods to construct good curves (i.e. curves with many points); for example:

1. Class field theory
2. Artin-Schreier and Kummer covers
3. Methods inspired by coding theory

Class Field Theory

Xing and Niederreiter have employed this with a lot of success. Their examples are not always explicit.

Here we give a simple explicit example where the structure of the class group is used.

Let C be the curve defined over \mathbf{F}_9 by the equation $y^3 - y = x + 1/x$, equivalently by

$$y^2 - (x^3 - x)y + 1 = 0.$$

Then $\#C(\mathbf{F}_9) = 20$ and $\text{Jac}(C)(\mathbf{F}_9) = \mathbf{Z}/15\mathbf{Z} \times \mathbf{Z}/15\mathbf{Z}$.

There is a subgroup of index 3 in $\text{Jac}(C)(\mathbf{F}_9)$ containing the differences

$$P_i - P_1 \quad \text{for } i = 1, \dots, 10$$

after suitable renumbering of the 20 points P_i . Hence there exists an unramified degree 3 cover \tilde{C} of C

$$g(\tilde{C}) = 4 \quad \#\tilde{C}(\mathbf{F}_9) = 30.$$

This is optimal. Similarly, a degree 9 cover D of C with

$$g(D) = 10 \quad \text{and} \quad \#D(\mathbf{F}_9) = 9 \times 6 = 54$$

(interval $[54 - 55]$).

Kummer Coverings (vdG-van der Vlugt)

We consider curves of the form $y^{q-1} = f$, where

1. f is not a d -th power in $\bar{\mathbf{F}}_q[X]$ for $1 < d|q-1$.
2. $f(x) = 1$ for many $x \in \mathbf{P}^1(\mathbf{F}_q)$.
3. f has many multiple zeros and poles.

The Hurwitz formula gives the genus. How to find f ?

Take a \mathbf{F}_p subspace L of \mathbf{F}_q with $\dim(L) = r$. We write

$$R = \prod_{c \in L} (X - c) = \sum a_i X^{p^i} \in \mathbf{F}_q.$$

and split R as

$$R = R_1 + R_2 = \sum_{i=s}^r b_i X^{p^i} + \sum_{i=0}^t c_i X^{p^i}$$

with $0 < s < r$, $t \leq s$, $b_r b_s \neq 0$ and $c_0 c_t \neq 0$. Zeros of R_i form space L_i .

Put

$$f = -R_1/R_2.$$

One has $f(x) = 1$ for $x \in L - (L_1 \cup L_2)$. Zeros of R_1 and ∞ have multiplicity > 1 .

$$g = \frac{1}{2} \left((p^{r-s} + p^t - \delta - 1)(q - 2) - \delta p^{(m,s)} - p^{(m,r-t)} + 2\delta + 2 \right)$$

and

$$\#C(\mathbf{F}_q) \geq (p^r - \delta)(q - 1)$$

where $r = \dim(L)$ and $\delta = \#(L_1 \cap L_2)$.

EXAMPLES. 1) \mathbf{F}_{16} . Take

$$R = X^{16} + X = \underbrace{X^{16} + X^2}_{R_1} + \underbrace{X^2 + X}_{R_2}.$$

The curve

$$y^{15} = (X^{16} + X^2)/(X^2 + X) = X^{14} + \dots + X.$$

has

$$g = 49 \quad \text{and} \quad \#C(\mathbf{F}_{16}) = 213.$$

(Compare the upper bound 286).

2) $q = p^m$ with m even.

$$C_m : \quad y^{q-1} = \frac{X^q - aX^{\sqrt{q}}}{aX^{\sqrt{q}} - X}$$

with $a \in \mathbf{F}_q^*$, and a not a $(\sqrt{q} - 1)$ th power. Then $g(C_m) = (\sqrt{q} - 1)(\sqrt{q} - 2) - \sqrt{q} + 2$ and $\#C_m(\mathbf{F}_q) = (q - 1)^2$.

$$q = 9, \quad g(C_m) = 13 \quad \text{and} \quad \#C_m(\mathbf{F}_9) = 64.$$

$$q = 81, \quad g(C_m) = 625, \quad \text{and} \quad \#C_m(\mathbf{F}_{81}) = 6400$$

Oesterlé upper bounds 66 and 7824.

A Method Using Coing Theory Let $R_q(s, m)$ be the q -ary Reed-Muller code:

$$P_s := \{f \in \mathbf{F}_q[X_1, \dots, X_m] : \deg(f) \leq s\}$$

then $R_q(s, m) = \text{Image}(\beta)$ with β evaluation map

$$\beta : P_s \rightarrow \mathbf{F}_q^n \quad (n = q^m), \quad f \mapsto (f(v))_{v \in \mathbf{F}_q^m}$$

Heijnen-Pellikaan: algorithm for determining minimum weight r -dimensional subcode.

Enumerate $\mathbf{F}_q = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$.

Set $Q = \{0, 1, \dots, q-1\}$. Order Q^m lexicographically.

An element $\sigma = (i_1, \dots, i_m)$ has degree $\deg(\sigma) = \sum_{j=1}^m i_j$.

$$\sigma \mapsto f = f_\sigma = \prod_{j=1}^m \prod_{t=i_j+1}^{q-1} (X_j - \alpha_t).$$

Take the first r elements of degree $\geq m(q-1) - s$, say $\sigma_1, \dots, \sigma_r$.

Then $\langle f_1, \dots, f_r \rangle$ is the required subspace with weight

$$d_r = 1 + \sum_{j=1}^m i_{m-j+1} q^{j-1}.$$

View now \mathbf{F}_{q^m} as a \mathbf{F}_q -vectorspace of dimension m with coordinates X_1, \dots, X_m .

For $a \in \mathbf{F}_{q^m}$ then $\text{Tr}(ax)$ is a linear form. ($\text{Tr} = \text{Tr}_{q^m/q}$) If a_1, \dots, a_m are \mathbf{F}_q -linearly independent then $\text{Tr}(a_1x), \dots, \text{Tr}(a_mx)$ can be viewed as coordinates X_1, \dots, X_m .

Substitute in f :

$$f = \prod_{j=1}^m \prod_{t=i_j+1}^{q-1} (\text{Tr}(a_jx) - \alpha_t)$$

Use now the identity

$$\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(\mathrm{Tr}(ax)bx) = \mathrm{Tr}\left(\sum_{j=0}^{m-1} a^{p^j} bx^{p^j+1}\right).$$

We can write

$$f = \mathrm{Tr}(R(x)) \quad \text{some } R \in \mathbf{F}_{q^m}[x].$$

The codeword is $c_f = \mathrm{Tr}(R(x))_{x \in \mathbf{F}_{q^m}}$. It defines a curve

$$X_f : y^q - y = R(x).$$

with $\#X_f(\mathbf{F}_q)$ given by the weight.

Example. We enumerate

$$\mathbf{F}_p = \{\alpha_0, \alpha_1, \dots, \alpha_{p-1}\} = \{p-1, p-2, \dots, 0\}.$$

and we consider $R_p(2, 3)$ for an odd prime p .

The first four elements $\sigma \in Q^m$ with degree $\geq 3(p-1) - 2 = 3p - 5$ are

$$(p-3, p-1, p-1), (p-2, p-2, p-1),$$

$$(p-2, p-1, p-2), (p-2, p-1, p-1).$$

The corresponding $f_i = \prod_{j=1}^m \prod_{t=i_j+1}^{q-1} (X_j - \alpha_t)$ are

$$f_1 = (X_1 - 1)X_1, \quad f_2 = X_1X_2, \quad f_3 = X_1X_3, \quad f_4 = X_1.$$

We get 3-dimensional subcode of $R_p(2, 3)$

$$\langle f_1, f_2, f_3 \rangle$$

with

$$d_3(R_p(2, 3)) = p^3 - p^2 - 1.$$

Using again

$$\mathrm{Tr}(ax)\mathrm{Tr}(bx) = \mathrm{Tr}(\mathrm{Tr}(ax)bx) = \mathrm{Tr}\left(\sum_{j=0}^{m-1} a^{p^j} b x^{p^j+1}\right).$$

repeatedly we can write

$$f_1 = \mathrm{Tr}(x^2 + x^{p+1} + x^{p^2+1}) - \mathrm{Tr}(x).$$

Since the trace map on \mathbf{F}_{p^3} satisfies

$$\mathrm{Tr}(x^{p^2+1}) = \mathrm{Tr}(x^{p+1})$$

we find for the corresponding codeword

$$c_{f_1} = \text{Tr}(2x^{p+1} + x^2 - x)_{x \in \mathbf{F}_{p^3}}.$$

The curve C_{f_1} associated to c_{f_1} is

$$y^p - y = 2x^{p+1} + x^2 - x.$$

From the number of zeros in c_{f_1} we immediately obtain

$$\#C_{f_1}(\mathbf{F}_{p^3}) = 2p^3 + 1,$$

and the genus satisfies

$$g(C_{f_1}) = (p - 1)p/2.$$

RESULT 1. For $p = 3$ we obtain a curve over \mathbf{F}_{27} of genus 3 with 55 points.

(Here 56 is optimal.)

PROPOSITION 1. The curve $C_{\mathcal{D}}$ defined over \mathbf{F}_{p^3} corresponding to $\mathcal{D} = \langle c_{f_1}, c_{f_2}, c_{f_3} \rangle$ has genus $(p^4 - p)/2$ and $\#C_{\mathcal{D}}(\mathbf{F}_{p^3}) = p^5 + p^3 + 1$.

PROPOSITION 2. The curve $C_{\mathcal{D}}$ defined over \mathbf{F}_{p^3} corresponding to the subcode $\mathcal{D} = \langle c_{f_1}, c_{f_2}, c_{f_3}, c_{f_4} \rangle$ has genus $(p^4 - p)p/2$ and $\#C_{\mathcal{D}}(\mathbf{F}_{p^3}) = p^6 + 1$.

EXAMPLE 1. For $p = 3$ the curve $C_{\mathcal{D}}$ over \mathbf{F}_{27} has

$$g = 117 \quad \text{and} \quad \#C_{\mathcal{D}}(\mathbf{F}_{27}) = 730.$$

Compare with Oesterlé's upper bound 859.

LINEAR EQUATIONS Let C be a curve over $k = \mathbf{F}_q$. Take a large set

$$\mathcal{P} \subset C(\mathbf{F}_q)$$

and a divisor D disjoint from \mathcal{P} . We choose a \mathbf{F}_p -vector space

$$F \subset L(D) = \{g \in \mathbf{F}_q(C) : (g) + D \geq 0\} \cup \{0\}$$

such that

1. $F \cap \{g^p - g : g \in k(C)\} = \{0\}$,
2. $\text{Tr}_{q/p}(f(P)) = 0$ for all $P \in \mathcal{P}$ and all $f \in F$.

An element $f \in k(C)$ defines the cover

$$C_f : z^p - z = f.$$

Let f_1, \dots, f_r be a basis of F and consider the fibre product of the $C_{f_i} : z_i^p - z_i = f_i$ with function field

$$K = k(C)(z_1, \dots, z_r).$$

EXAMPLE. Take the elliptic curve C/\mathbf{F}_3 defined by

$$y^3 - y = x^2 - 1 \quad \text{with} \quad \#C(\mathbf{F}_3) = 7.$$

Let $P_\infty = (0 : 1 : 0)$, $Q = (1, 0)$ and set

$$D = 8P_\infty + 2Q.$$

We consider a suitable subspace \tilde{W} of $L(D)$ with basis:

$$1, (y + 2)/(2x + y + 1), (x + y + 1)/y, y, \\ x + 2, y^2, (x + 2)y, (x + 2)y^2, (x + 2)^2y.$$

We solve in \tilde{W} for the remaining 5 rational points P_i of C

$$\mathrm{Tr}_{3/3}(f(P_i)) = f(P_i) = 0 \quad i = 1, \dots, 5$$

and we get a 4-dimensional space F generated by

$$\begin{aligned} f_1 &= (y + 2)/(2x + y + 1) + y + x + y^2, \\ f_2 &= (y + 2)/(2x + y + 1) + (x + y + 1)/y + x + 2xy, \\ f_3 &= 2 + (y + 2)/(2x + y + 1) + y + 2y^2 + xy^2, \\ f_4 &= 2y + x^2y \end{aligned}$$

with the following curves $y^3 - y = f_i$

$f_i =$	$g(C_{f_i})$	$\#C_{f_i}(\mathbf{F}_3)$
f_1	9	17
f_2	10	17
f_3	12	17
f_4	10	19

Analyzing the subspaces of F we get:

F	$g(C_F)$	$\#C_F(\mathbf{F}_3)$	$N_q(g)$
$\langle f_1, f_2 \rangle$	35	47	[47 – 51]
$\langle f_1 + 2f_3, f_4 \rangle$	36	46	[48 – 52]
$\langle f_1, f_3 \rangle$	39	46	[46 – 56]
$\langle f_1, f_2, f_3 \rangle$	128	136	[136 – 149]

Table p=2.

$g \backslash q$	2	4	8	16	32	64	128
1	5	9	14	25	44	81	150
2	6	10	18	33	53	97	172
3	7	14	24	38	64	113	192
4	8	15	25	45	71-74	129	215
5	9	17	29-30	49-53	83-85	132-145	227-234
6	10	20	33-35	65	86-96	161	243-258
7	10	21-22	34-38	63-69	98-107	177	262-283
8	11	21-24	35-42	62-75	97-118	169-193	276-302
9	12	26	45	72-81	108-128	209	288-322
10	13	27	42-49	81-87	113-139	225	296-345
11	14	26-29	48-53	80-91	120-150	201-236	294-366
12	14-15	29-31	49-57	83-97	129-161	257	321-388
13	15	33	56-61	97-102	129-172	225-268	
14	15-16	32-35	65	97-107	146-183	241-284	353-437
15	17	33-37	57-67	98-113	158-194	258-300	386-455
16	17-18	36-38	56-71	95-118	147-204	267-316	
17	17-18	40	63-74	112-123	154-212		
18	18-19	41-42	65-77	113-129	161-220	281-348	
19	20	37-43	60-80	129-134	172-228	315-364	
20	19-21	40-45	68-83	127-139	177-236	297-380	
21	21	41-47	72-86	129-145	185-243	281-396	
22	21-22	42-48	74-89	129-150		321-412	
23	22-23	45-50	68-92	126-155			
24	21-23	49-52	81-95	129-161	225-267	337-444	513-653
25	24	51-53	86-97	144-165		335-460	
26	24-25	55	82-100	150-171		385-476	
27	24-25	50-56	96-103	145-176	213-290	401-492	
28	25-26	53-58	97-106	145-181	257-298	513	577-745
29	25-27	52-60	97-109	161-186	227-305		
30	25-27	53-61	96-112	162-191	273-313	401-535	609-784

For references see

<http://www.science.uva.nl/~geer>

Next Update January 2006.