Even sharper upper bounds on the number of points on curves

Everett W. Howe

Center for Communications Research, La Jolla

Symposium on Algebraic Geometry and its Applications
Tahiti, May 2007
Revised slides
How many points can there be on a genus-$g$ curve?

For a prime power $q$ and an integer $g \geq 0$, set

$$N_q(g) = \max \{ \# C(\mathbb{F}_q) : C \text{ is a genus-}g \text{ curve over } \mathbb{F}_q \}.$$ 

Questions

What can we say about $N_q(g)$ . . .

- Asymptotically?
- For specific values of $q$ and $g$?
Asymptotic results ($q$ fixed, $g \to \infty$).

We set $A(q) = \limsup_{g \to \infty} N_q(g)/g$.

**Weil**

We have $N_q(g) \leq q + 1 + 2g\sqrt{q}$, so $A(q) \leq 2\sqrt{q}$.

**Serre**

We have $N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor$, so $A(q) \leq \lfloor 2\sqrt{q} \rfloor$.

**Ihara**

We have $A(q) \leq (\sqrt{8q + 1} - 1)/2$.

**Drinfel’d-Vlăduț**

We have $A(q) \leq \sqrt{q} - 1$, with equality when $q$ is square.
Specific values of $q$ and $g$.

Goal: Find upper and lower bounds on $N_q(g)$.

### Lower bounds

Clever people construct curves with many points, using . . .

- Class field theory
- Towers of curves
- Fiber products of Artin-Schreier curves
- Modular curves
- Other explicit curves
- . . .

Many, many people have contributed to the best known lower bounds for various $q$ and $g$. 
Specific values of $q$ and $g$.

Upper bounds

- Weil-Serre bound
- Oesterlé bound
- Other restrictions (Stöhr-Voloch, Fuhrmann-Torres, Korchmáros-Torres, ...)

Are these upper bounds on $N_q(g)$ the best possible?

Or can we sometimes do better?
The **Weil polynomial** of an abelian variety $A$ over $\mathbb{F}_q$ is the characteristic polynomial of its Frobenius endomorphism.

The **Weil polynomial** of curve over $\mathbb{F}_q$ is the Weil polynomial of its Jacobian.

If $A$ has dimension $n$, then its Weil polynomial has the form

$$x^{2n} + a_1 x^{2n-1} + \cdots + a_{n-1} x^{n+1} + a_n x^n + a_{n-1} q x^{n-1} + \cdots + a_1 q^{2n-1} x + q^{2n}.$$ 

All of its roots in $\mathbb{C}$ lie on the circle $|z| = \sqrt{q}$. Its real roots have even multiplicity.

**Note:** The Honda-Tate theorem provides further restrictions.
More on Weil polynomials.

Since the roots of $f$ come in complex-conjugate pairs, we may write

$$f(x) = x^n h(x + q/x)$$

for a unique monic $h \in \mathbb{Z}[x]$, the real Weil polynomial of $C$. The roots of $h$ are real numbers in the interval $[-2\sqrt{q}, 2\sqrt{q}]$.

Note that if $f = x^{2n} + a_1 x^{2n-1} + \cdots$, then $h = x^n + a_1 x^{n-1} + \cdots$.

**Theorem (Tate)**

*Two abelian varieties over $\mathbb{F}_q$ are isogenous to one another if and only if they have the same Weil polynomial.*
Suppose $C$ is a genus-$g$ curve over $\mathbb{F}_q$, with Weil polynomial $f$. Write $f = \prod_{i=1}^{2g} (x - \pi_i)$ with $\pi_i \in \mathbb{C}$. Then for all $d > 0$ we have

$$\# C(\mathbb{F}_{q^d}) = q^d + 1 - \sum \pi_i^d.$$ 

In particular, if $f = x^{2g} + a_1 x^{2g-1} + \cdots$, then

$$\# C(\mathbb{F}_q) = q + 1 + a_1.$$ 

These formulas can be used to compute the number of degree-$d$ places on the curve, for each $d$. 

Weil polynomials of curves.
Serre’s strategy for bounding $N_q(g)$.

Goal: Show that no genus-$g$ curve over $\mathbb{F}_q$ has exactly $N$ points.

- Compute all $h = x^g + a_1 x^{g-1} + \cdots$ with all complex roots in the real interval $[-2\sqrt{q}, 2\sqrt{q}]$, where $a_1 = N - q - 1$.
- Find a reason why each $h$ can’t come from a curve.
  - The Honda-Tate conditions.
  - The number of degree-$d$ places on a curve must be $\geq 0$.
  - The “resultant 1” method.
    - Eliminate $h$ if $h = h_1 h_2$ with $\text{Res}(h_1, h_2) = 1$.
  - Restrictions when $h$ is the real Weil polynomial of $E^g$.
  - Miscellaneous ad hoc methods.
Extensions to Serre’s techniques.

In 2003, Kristin Lauter and I added some further methods:

- **The “resultant 2” method.**
  - If $h = h_1 h_2$ and $\text{Res}(\sqrt{h_1}, \sqrt{h_2}) = 2$, then $C$ must be a double cover of a curve with real Weil polynomial $h_1$ or $h_2$.
  - (Here $\sqrt{h_i}$ denotes the **radical** of $h_i$.)

- **The “elliptic factor” method.**
  - If $h = (x - t)h_2$ for the real Weil polynomial $x - t$ of an elliptic curve $E$, and if $r = \text{Res}(x - t, \sqrt{h_2})$, then $C$ has a map of degree dividing $r$ to an elliptic curve isogenous to $E$.

Sometimes, contradictions follow.
Example.

Consider \( q = 8, \ g = 9, \ N = 46 \).

Let \( h = (x + 3)^4(x + 5)^5 \). All of its roots lie in \([-2\sqrt{8}, 2\sqrt{8}]\). Why isn’t it the real Weil polynomial of a genus-9 curve \( C \) over \( \mathbb{F}_8 \)?

Answer: The resultant 2 method.

Such a \( C \) would be a double cover of a curve with real Weil polynomial either \( (x + 3)^4 \) or \( (x + 5)^5 \).

A curve with real Weil polynomial \( (x + 5)^5 \) would have fewer points over \( \mathbb{F}_{64} \) than over \( \mathbb{F}_8 \), so \( (x + 5)^5 \) fails.

A curve with real Weil polynomial \( (x + 3)^4 \) has 21 points. A curve with 46 points can’t be a double cover of a curve with 21 points.
The van der Geer/van der Vlugt tables

Upper and lower bounds on $N_q(g)$, as of January 2002.

<table>
<thead>
<tr>
<th>$g \ \backslash \ q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45 – 46</td>
<td>71 – 75</td>
<td>129</td>
<td>215 – 217</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33 – 35</td>
<td>65</td>
<td>86 – 97</td>
<td>161</td>
<td>243 – 261</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21 – 22</td>
<td>34 – 39</td>
<td>63 – 70</td>
<td>98 – 108</td>
<td>177</td>
<td>258 – 283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45 – 47</td>
<td>72 – 81</td>
<td>108 – 130</td>
<td>209</td>
<td>288 – 327</td>
</tr>
</tbody>
</table>
The van der Geer/van der Vlugt tables

Upper bounds from 2002, lower bounds from November 2006.

<table>
<thead>
<tr>
<th>$g \backslash q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45–46</td>
<td>71–75</td>
<td>129</td>
<td>215–217</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33–35</td>
<td>65</td>
<td>86–97</td>
<td>161</td>
<td>243–261</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21–22</td>
<td>34–39</td>
<td>63–70</td>
<td>98–108</td>
<td>177</td>
<td>262–283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45–47</td>
<td>72–81</td>
<td>108–130</td>
<td>209</td>
<td>288–327</td>
</tr>
</tbody>
</table>

Everett W. Howe
Upper and lower bounds on $N_q(g)$, as of November 2006.

<table>
<thead>
<tr>
<th>$g \setminus q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>71</td>
<td>74</td>
<td>129</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>17</td>
<td>29</td>
<td>30</td>
<td>49</td>
<td>53</td>
<td>83</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33</td>
<td>35</td>
<td>65</td>
<td>86</td>
<td>96</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21</td>
<td>22</td>
<td>34</td>
<td>38</td>
<td>63</td>
<td>69</td>
</tr>
<tr>
<td>8</td>
<td>11</td>
<td>21</td>
<td>24</td>
<td>35</td>
<td>42</td>
<td>62</td>
<td>75</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45</td>
<td>45</td>
<td>72</td>
<td>81</td>
<td>108</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>27</td>
<td>27</td>
<td>42</td>
<td>49</td>
<td>81</td>
<td>87</td>
</tr>
<tr>
<td>11</td>
<td>14</td>
<td>26</td>
<td>29</td>
<td>48</td>
<td>53</td>
<td>80</td>
<td>91</td>
</tr>
<tr>
<td>12</td>
<td>14</td>
<td>15</td>
<td>29</td>
<td>31</td>
<td>49</td>
<td>57</td>
<td>88</td>
</tr>
<tr>
<td>13</td>
<td>15</td>
<td>33</td>
<td>56</td>
<td>61</td>
<td>97</td>
<td>102</td>
<td>129</td>
</tr>
<tr>
<td>14</td>
<td>15</td>
<td>16</td>
<td>32</td>
<td>35</td>
<td>65</td>
<td>97</td>
<td>107</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
<td>35</td>
<td>37</td>
<td>57</td>
<td>67</td>
<td>98</td>
<td>113</td>
</tr>
</tbody>
</table>
The van der Geer/van der Vlugt tables

Upper and lower bounds on $N_q(g)$, as of November 2006.

<table>
<thead>
<tr>
<th>$g \setminus q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>71–74</td>
<td>129</td>
<td>215</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33–35</td>
<td>65</td>
<td>86–96</td>
<td>161</td>
<td>243–258</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21–22</td>
<td>34–38</td>
<td>63–69</td>
<td>98–107</td>
<td>177</td>
<td>262–283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45</td>
<td>72–81</td>
<td>108–128</td>
<td>209</td>
<td>288–322</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>27</td>
<td>42–49</td>
<td>81–87</td>
<td>113–139</td>
<td>225</td>
<td>296–345</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
<td>35–37</td>
<td>57–67</td>
<td>98–113</td>
<td>158–194</td>
<td>258–300</td>
<td>386–455</td>
</tr>
</tbody>
</table>
New methods.

Lauter and I have been revisiting this topic.

New methods

- The “reduced resultant 2” method.
- The “generalized elliptic factor” method.

Rest of the talk:

- Explain the new (and old) methods.
- Show some new results.
The basic idea.

Question underlying the old and new methods:
How close is Jac $C$ to a product of polarized varieties?

Suppose $h$ is the real Weil polynomial of an isogeny class $\mathcal{I}$.

If $h = h_1 h_2$ for two coprime factors, then $\mathcal{I}$ contains $A_1 \times A_2$, where $\text{Hom}(A_1, A_2) = 0$.

(The real Weil polynomial for $A_i$ is $h_i$.)
Finding the smallest kernel.

\[ 0 \rightarrow \Delta' \rightarrow A_1 \times A_2 \rightarrow \text{Jac } C \rightarrow 0 \]
Finding the smallest kernel.

\[
\begin{array}{ccc}
\Delta_1 \times \Delta_2 & \longrightarrow & \Delta_1 \times \Delta_2 \\
\downarrow & & \downarrow \\
\Delta' & \longrightarrow & A_1 \times A_2 \\
\downarrow & & \downarrow \\
0 & \longrightarrow & \text{Jac } C & \longrightarrow & 0 \\
\end{array}
\]
Finding the smallest kernel.

\[
\begin{align*}
\Delta_1 \times \Delta_2 & \longrightarrow \Delta_1 \times \Delta_2 \\
0 & \longrightarrow \Delta' \longrightarrow A_1 \times A_2 \longrightarrow \text{Jac } C \longrightarrow 0 \\
0 & \longrightarrow \Delta \longrightarrow B_1 \times B_2 \longrightarrow \text{Jac } C \longrightarrow 0
\end{align*}
\]
Finding the smallest kernel.

Each $B_i$ is the image of $A_i$ in $\text{Jac } C$.

Projections $B_1 \times B_2 \to B_i$ give injections $\Delta \hookrightarrow B_1$ and $\Delta \hookrightarrow B_2$.

Goal: Understand $\Delta$. 
Bounding the size of the kernel $\Delta$.

Let $\pi, \pi_1, \pi_2$ be Frobenius on $\text{Jac } C, B_1, B_2$, respectively.

\[
\begin{align*}
\text{End } \text{Jac } C & \xrightarrow{} (\text{End } B_1) \times (\text{End } B_2) \\
\mathbb{Z}[\pi, \overline{\pi}] & \xrightarrow{} \mathbb{Z}[\pi_1, \overline{\pi}_1] \times \mathbb{Z}[\pi_2, \overline{\pi}_2] \\
\pi & \xrightarrow{} (\pi_1, \pi_2)
\end{align*}
\]
Bounding the size of the kernel $\Delta$.

Let $\pi, \pi_1, \pi_2$ be Frobenius on $\text{Jac } C, B_1, B_2$, respectively.

End $\text{Jac } C \xrightarrow{\pi} (\text{End } B_1) \times (\text{End } B_2)$

$\mathbb{Z}[\pi, \pi] \xrightarrow{\pi} \mathbb{Z}[\pi_1, \pi_1] \times \mathbb{Z}[\pi_2, \pi_2]$  

Find $\varphi$ such that $\varphi \xrightarrow{} (0, n)$ for some $n$. 
Bounding the size of the kernel $\Delta$.

Let $\pi, \pi_1, \pi_2$ be Frobenius on $\text{Jac } C, B_1, B_2$, respectively.

End $\text{Jac } C \longrightarrow (\text{End } B_1) \times (\text{End } B_2)$

$\mathbb{Z}[\pi, \pi] \longrightarrow \mathbb{Z}[\pi_1, \pi_1] \times \mathbb{Z}[\pi_2, \pi_2]$

$\pi \longmapsto (\pi_1, \pi_2)$

Find $\varphi$ such that $\varphi \longmapsto (0, n)$ for some $n$.

Then $\varphi$ acts as 0 on $B_1 \leftrightarrow \Delta$, and $\varphi$ acts as $n$ on $B_2 \leftrightarrow \Delta$, so $\Delta$ is killed by $n$. 
A simpler computation.

\[
\mathbb{Z}[\pi, \bar{\pi}] \hookrightarrow \mathbb{Z}[\pi_1, \bar{\pi}_1] \times \mathbb{Z}[\pi_2, \bar{\pi}_2]
\]

Find \( n > 0 \) for which there is a \( \varphi \in \mathbb{Z}[\pi + \bar{\pi}] \) that maps to \((0, n)\).

Let \( m_i = (\text{minimal polynomial of } \pi_i + \bar{\pi}_i) = \sqrt{h_i}. \)

\[
\mathbb{Z}[x]/(m_1 m_2) \hookrightarrow \mathbb{Z}[x]/(m_1) \times \mathbb{Z}[x]/(m_2)
\]

Smallest \( n \) is the generator of the ideal \( \mathbb{Z} \cap (m_1, m_2). \)
Reduced resultants.

**Definition**

The *reduced resultant* $\text{Res}'(f, g)$ of two polynomials $f, g \in \mathbb{Z}[x]$ is the non-negative generator of the ideal $\mathbb{Z} \cap (f, g)$.

To compute $\text{Res}'(f, g)$:
Write $af + bg = 1$ in $\mathbb{Q}[x]$, and then clear denominators.

The reduced resultant divides the usual resultant, and is divisible by the radical of the usual resultant.

**Note**

The $n$ we get from $\mathbb{Z}[\pi, \bar{\pi}]$ is either $\text{Res}'(m_1, m_2)$ or half this, and we can easily tell which.

The $n$ we get from $\mathbb{Z}[\pi, \bar{\pi}]$ is the *modified reduced resultant*. 

Everett W. Howe
Upper bounds on the number of points on curves 18
New versions of old results.

Let $h = h_1 h_2$ be the real Weil polynomial of an isogeny class $\mathcal{I}$, where $h_1$ and $h_2$ are coprime.

Let $r$ be the modified reduced resultant of $\sqrt{h_1}$ and $\sqrt{h_2}$.

**Theorem (Serre)**

*If $r = 1$ then there is no Jacobian in $\mathcal{I}$.***

**Theorem**

*If $r = 2$ and if Jac $C$ lies in $\mathcal{I}$, then $C$ is a double cover of a curve $D$ whose real Weil polynomial is either $h_1$ or $h_2$.***
Proof.

Consider the principal polarization $\lambda$ on $\text{Jac } C$.

$$\text{Jac } C \xrightarrow{\sim} \hat{\text{Jac } C}$$
Proof.

Consider the principal polarization $\lambda$ on $\text{Jac } C$.

$B_1 \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{B}_1 \times \hat{B}_2$

$\downarrow \quad \quad \downarrow$

$\text{Jac } C \xrightarrow{\lambda} \hat{\text{Jac } C}$

If $r = 1$ . . .

Then $(\text{Jac } C, \lambda) \sim (B_1 \times B_2, \mu_1 \times \mu_2)$, impossible.

If $r = 2$ . . .

Consider the involution $(1, -1)$ of $(B_1 \times B_2, \mu_1 \times \mu_2)$:

acts trivially on $\Delta$;

gives an involution of $(\text{Jac } C, \lambda)$;

gives an involution of $C$, and so a double cover $C \rightarrow D$. 

Everett W. Howe

Upper bounds on the number of points on curves
Proof.

Consider the principal polarization $\lambda$ on $\text{Jac} \, C$.

If $r = 1 \ldots$

Then $(\text{Jac} \, C, \lambda) \cong (B_1 \times B_2, \mu_1 \times \mu_2)$, impossible.
Proof.

Consider the principal polarization $\lambda$ on $\text{Jac } C$.

$$\begin{array}{c}
B_1 \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{B}_1 \times \hat{B}_2 \\
\downarrow \downarrow \\
\text{Jac } C \xrightarrow{\lambda} \text{Jac } C
\end{array}$$

**If $r = 1$ . . .**

Then $(\text{Jac } C, \lambda) \cong (B_1 \times B_2, \mu_1 \times \mu_2)$, impossible.

**If $r = 2$ . . .**

Consider the involution $(1, -1)$ of $(B_1 \times B_2, \mu_1 \times \mu_2)$:

- acts trivially on $\Delta$;
- gives an involution of $(\text{Jac } C, \lambda)$;
- gives an involution of $C$, and so a double cover $C \to D$. 

Everett W. Howe

Upper bounds on the number of points on curves
The generalized elliptic factor method.

Suppose $\mathcal{I}$ contains $E^n \times A$, where $\text{Hom}(E, A) = 0$.

Gives $h = h_1 h_2$ with $h_1 = (x - t)^n$, where $t = \text{trace}(E)$.

Let $r$ be the modified reduced resultant of $\sqrt{h_1}$ and $\sqrt{h_2}$.

**Theorem**

Suppose $\text{Jac } C$ lies in $\mathcal{I}$.

- If $n = 1$, then there is a map from $C$ to an elliptic curve isogenous to $E$, of degree dividing $r$.
- If $n > 1$, then there is a map from $C$ to an elliptic curve isogenous to $E$, whose degree can be effectively bounded.
Sketch of proof.

Recall that in general we had

\[
B_1 \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{B}_1 \times \hat{B}_2
\]

\[
\downarrow \quad \downarrow
\]

\[
\text{Jac } C \xrightarrow{\sim} \lambda \xrightarrow{\sim} \text{Jac } C
\]

where the kernel $\Delta$ of $B_1 \times B_2 \to \text{Jac } C$ injects into $B_1$ and $B_2$.

Then $\Delta \hookrightarrow \ker \mu_1$ and $\Delta \hookrightarrow \ker \mu_2$ as well.

Counting degrees, we find that $\ker \mu_1 \cong \Delta \cong \ker \mu_2$.

In present case $B_1 \sim E^n$. 
Sketch of proof, $n = 1$. 

\[
\begin{array}{c}
F \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{F} \times \hat{B}_2 \\
\downarrow \quad \downarrow \\
\text{Jac } C\xrightarrow{\sim} \text{Jac } C \\
\end{array}
\]
Sketch of proof, \( n = 1 \).
Sketch of proof, $n = 1$. 

\[ F \xrightarrow{\mu_1} \hat{F} \]

\[ \text{Jac } C \xrightarrow{\sim} \text{Jac } C \]
Sketch of proof, $n = 1$. 

\[ F \xrightarrow{\mu_1} \hat{F} \xrightarrow{} F \]

\[ C \xrightarrow{} \text{Jac } C \xrightarrow{\sim} \hat{\text{Jac } C} \]
Sketch of proof, $n = 1$. 

\[ F \xrightarrow{\mu_1} \hat{F} \xrightarrow{\varphi} F \]

\[ C \xrightarrow{\lambda} \overset{\sim}{\text{Jac}} C \]
Sketch of proof, $n = 1$.

\[ F \xrightarrow{\mu_1} \hat{F} \xrightarrow{(\deg \varphi)\lambda_F} F \]

\[ C \xrightarrow{\varphi^*} \text{Jac } C \xrightarrow{\lambda} \tilde{\text{Jac } C} \]

$\mu_1$ is multiplication-by-$\deg \varphi$, followed by canonical polarization.

Since kernel $\mu_1$ is killed by $r$, $\deg \varphi$ divides $r$. 
Recall the statement we want to prove:

We have:
- $h = h_1 h_2$ with $h_1 = (x - t)^n$, where $t = \text{trace}(E)$.
- $n > 1$.
- $r$ is the modified reduced resultant of $(x - t)$ and $\sqrt{h_2}$.
- A curve $C$ has real Weil polynomial $h_1 h_2$.

We want to show:
- There is a map from $C$ to an elliptic curve isogenous to $E$, whose degree can be effectively bounded.
Sketch of proof, $n > 1$.

Let us consider the case where $t^2 - 4q$ is a fundamental discriminant, corresponding to a quadratic order $\mathcal{O}$ of class number 1.

Then $B_1 \cong E^n$, and a polarization $\mu_1$ on $B_1$ can be viewed as a positive definite Hermitian form $H$ on $\mathcal{O}^n$.

We have $\deg \mu_1 = (\det \text{Gram } H)^2$.

Suppose $\gamma = (a_1, a_2, \ldots, a_n) \in \mathcal{O}^n$ has squared-length $m$ under $H$.

Consider the map $\Gamma : E \to E^n$ given by $\gamma$. Then the pullback of $\mu_1$ by $\Gamma$ is $m$ times the canonical polarization of $E$. 
The big diagram when $n > 1$.

\[ E^n \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{E}^n \times \hat{B}_2 \]

\[ \text{Jac } C \xrightarrow{\lambda} \text{Jac } C \]
The big diagram when $n > 1$. 

\[ E^n \xrightarrow{\mu_1} \hat{E}^n \]
\[ E^n \times B_2 \xrightarrow{\mu_1 \times \mu_2} \hat{E}^n \times \hat{B}_2 \]
\[ \text{Jac } C \xrightarrow{\lambda} \hat{\text{Jac } C} \]

We need bounds on the length of the shortest vector in a Hermitian lattice with a given Gram determinant.
The big diagram when \( n > 1 \).

\[ E^n \xrightarrow{\mu_1} \hat{E}^n \]

\[ \text{Jac } C \xrightarrow{\lambda} \sim \text{Jac } C \]
The big diagram when $n > 1$.

\[
\begin{array}{c}
E \\
\downarrow \Gamma \ \\
E^n \\
\downarrow \mu_1 \\
\text{Jac } C
\end{array}
\quad \xrightarrow{\text{degree } m^2} \quad
\begin{array}{c}
\hat{E} \\
\downarrow \hat{\Gamma} \ \\
\hat{E}^n \\
\downarrow \lambda \\
\text{Jac } C
\end{array}
\]
The big diagram when \( n > 1 \).
The big diagram when $n > 1$. 

\[ E \xrightarrow{\text{degree } m^2} \hat{E} \xrightarrow{} E \]

\[ C \xrightarrow{} \text{Jac } C \xrightarrow{\lambda} \sim \xrightarrow{} \text{Jac } C \]
So $\deg \varphi = m$. We need bounds on the length of the shortest vector in a Hermitian lattice with a given Gram determinant.
Possible real Weil polynomial for $q = 4$, $g = 7$, $N = 22$: $h = h_1 h_2$ with $h_1 = (x + 3)^3$ and $h_2 = x(x + 2)^2(x + 4)$.

Let $E$ have real Weil polynomial $x + 3$. $E$ has complex multiplication by $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-7})/2]$.

We deduce... 
- a polarization of degree 9 on $E^3$; and therefore 
- a Hermitian form $H$ on $\mathcal{O}^3$ with $\det \text{Gram } H = 3$.

If $H$ has vector of squared-length 2, we get double cover $C$ (with 22 points) $\rightarrow E$ (with 8 points), contradiction.

Note: Vector of squared-length 3 doesn’t help us.
From a Hermitian form to a positive quadratic form.

View $\mathcal{O}$ as $\mathbb{Z} \oplus \mathbb{Z}$. Then $H$ gives us an integer-valued positive definite quadratic form $P$ on $\mathbb{Z}^6$.

(Note: The associated bilinear form is the real part of $H$, which is half-integer valued.)

- $\det \text{Gram } P = N_{\mathcal{O}/\mathbb{Z}}(\det \text{Gram } H) \cdot |\text{disc } \mathcal{O}/4|^3 = 3087/64$.
- Let $M_1, \ldots, M_6$ be successive minima of $P$. Then

  $$M_1 \cdots M_6 \leq (64/3)(3087/64) = 1029.$$

- If no vectors of squared-length 1 or 2, then

  $$M_1 = M_2 = M_3 = M_4 = M_5 = 3 \quad \text{and} \quad 3 \leq M_6 \leq 4.$$
Back to the Hermitian form.

The first 5 minima generate a $\mathbb{Q}$-vector space of dimension 5. So they must generate a $\mathbb{Q}(\sqrt{-7})$-vector space of dimension 3.

Let $v_1, v_2, v_3 \in \mathcal{O}^3$ be $\mathbb{Q}(\sqrt{-7})$-independent vectors of squared-length 3.

Let $\Lambda$ be $\mathcal{O}$-sublattice of $\mathcal{O}^3$ generated by $v_1, v_2, v_3$.

\[
\text{Gram } H|_{\Lambda} = \begin{bmatrix} 3 & a & b \\ \bar{a} & 3 & c \\ \bar{b} & \bar{c} & 3 \end{bmatrix}
\]

\[
\det \text{Gram } H|_{\Lambda} = (\det \text{Gram } H) \cdot N_{\mathcal{O}/\mathbb{Z}}([\mathcal{O}^3/\Lambda]).
\]

positive definite $\implies$ $a, b, c$ have norm less than 9.
A small finite problem.

Algorithm to find bad forms:

- Enumerate all possible \((a, b, c)\).
- For each triple: Does associated matrix have determinant \(3N(\mathcal{A})\) for an ideal \(\mathcal{A}\) of \(\mathcal{O}\)?
- If so, find all superlattices on which form has determinant 3.
- Compute shortest vector \(v\) in each superlattice.
- If \(v\) has squared-length 3, we have a bad example.

We found no bad examples.

Every polarization of degree 9 on \(E^3\) can be pulled back to a polarization of degree 1 or 4 on \(E\).
Remark.

This procedure does not scale well to higher dimensions.

When $\det \text{Gram } H$ is a norm from $\mathcal{O}$, there is a better procedure.

- Based on Schiemann’s calculation of all unimodular forms on $\mathcal{O}^n$ for small $n$ and small $\mathcal{O}$.
- When $\det \text{Gram } H$ is a norm, there is a superlattice on which $H$ is unimodular.
Sample optimal bounds.

For the quadratic order $\mathcal{O}$ of discriminant $-7$:

<table>
<thead>
<tr>
<th>dim \ det</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Sharp upper bounds on the squared-lengths of short vectors for Hermitian forms over $\mathcal{O}$ of a given dimension and determinant.
Computer calculations.

Pari/GP code

- Given $q$, $g$, $N$, enumerates all polynomials $h$ with
  - leading terms $x^g + (N - q - 1)x^{g-1} + \cdots$, and
  - all complex roots in $[-2\sqrt{q}, 2\sqrt{q}]$.
  - Uses ideas of McKee and Smyth (ANTS 2004).
- Eliminates those that are not Weil polynomials.
- Computes all possible splittings $h = h_1 h_2$.
  - Computes modified reduced resultant of each splitting.
- Applies Serre’s “reduced resultant 1” criterion.
- Applies “reduced resultant 2” method.
- Applies generalized elliptic factor method.
- If either method gives a cover $C \to D$, checks some conditions to see whether such a cover is possible.
New results.

Upper and lower bounds on $N_q(g)$, as of November 2006.

<table>
<thead>
<tr>
<th>$g \setminus q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>71–74</td>
<td>129</td>
<td>215</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33–35</td>
<td>65</td>
<td>86–96</td>
<td>161</td>
<td>243–258</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21–22</td>
<td>34–38</td>
<td>63–69</td>
<td>98–107</td>
<td>177</td>
<td>262–283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45</td>
<td>72–81</td>
<td>108–128</td>
<td>209</td>
<td>288–322</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>27</td>
<td>42–49</td>
<td>81–87</td>
<td>113–139</td>
<td>225</td>
<td>296–345</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
<td>35–37</td>
<td>57–67</td>
<td>98–113</td>
<td>158–194</td>
<td>258–300</td>
<td>386–455</td>
</tr>
</tbody>
</table>
New results.

Current upper bounds, lower bounds from November 2006.

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>71 – 72</td>
<td>129</td>
<td>215</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33 – 34</td>
<td>65</td>
<td>86 – 96</td>
<td>161</td>
<td>243 – 258</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21 – 21</td>
<td>34 – 38</td>
<td>63 – 69</td>
<td>98 – 107</td>
<td>177</td>
<td>262 – 283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45</td>
<td>72 – 81</td>
<td>108 – 128</td>
<td>209</td>
<td>288 – 322</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>27</td>
<td>42 – 49</td>
<td>81 – 87</td>
<td>113 – 139</td>
<td>225</td>
<td>296 – 345</td>
</tr>
</tbody>
</table>
New results.

Current upper bounds, lower bounds from November 2006.

<table>
<thead>
<tr>
<th>$g \setminus q$</th>
<th>2</th>
<th>4</th>
<th>8</th>
<th>16</th>
<th>32</th>
<th>64</th>
<th>128</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>9</td>
<td>14</td>
<td>25</td>
<td>44</td>
<td>81</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>10</td>
<td>18</td>
<td>33</td>
<td>53</td>
<td>97</td>
<td>172</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>14</td>
<td>24</td>
<td>38</td>
<td>64</td>
<td>113</td>
<td>192</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>15</td>
<td>25</td>
<td>45</td>
<td>71 – 72</td>
<td>129</td>
<td>215</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>17</td>
<td>29</td>
<td>49 – 53</td>
<td>83 – 85</td>
<td>132 – 145</td>
<td>227 – 234</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
<td>20</td>
<td>33 – 34</td>
<td>65</td>
<td>86 – 96</td>
<td>161</td>
<td>243 – 258</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
<td>21</td>
<td>34 – 38</td>
<td>63 – 69</td>
<td>98 – 107</td>
<td>177</td>
<td>262 – 283</td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td>26</td>
<td>45</td>
<td>72 – 81</td>
<td>108 – 128</td>
<td>209</td>
<td>288 – 322</td>
</tr>
<tr>
<td>10</td>
<td>13</td>
<td>27</td>
<td>42 – 49</td>
<td>81 – 87</td>
<td>113 – 139</td>
<td>225</td>
<td>296 – 345</td>
</tr>
</tbody>
</table>
Tempting partial results.

Genus-12 curves over $\mathbb{F}_2$ with 15 points:

- Code examined 22 possible polynomials.
  - All satisfied Honda-Tate conditions.
  - 10 failed “reduced resultant 1” test.
  - 7 failed “reduced resultant 2” test.
  - None failed “generalized elliptic factor” test.
  - 3 were eliminated by \textit{ad hoc} methods.

Only two possible real Weil polynomials:

- $(x + 1)^2(x + 2)^2(x^2 - 2)(x^2 + 2x - 2)^3$
- $(x^2 + x - 3)(x^3 + 3x^2 - 3)(x^3 + 4x^2 + 3x - 1)(x^4 + 4x^3 + 2x^2 - 5x - 3)$

First has degree-4 map to elliptic curve with 4 points.
Second has $\mathbb{F}_{2^7}$-rational degree-4 map to elliptic curve over $\mathbb{F}_2$ with 2 points.