Theorem 1. *Let $C(p, f)$ be the Artin-Schreier curve over $\mathbf{F}_p$ defined by the affine equation*

$$y^d = x^p - x \qquad \text{where } d = p^f - 1.$$

(Assume that $f > 1$ when $p = 2$.) Then its Jacobian has a 1-dimensional formal summand of height $(p-1)f$.

Properties of $C(p, f)$:

- Its genus is $(p-1)(d-1)/2$.
- It has an action by the group

  $$\tilde{G} = \mathbf{F}_p \rtimes \mu_{(p-1)d}$$

  given by

  $$(x, y) \mapsto (\zeta^d x + a, \zeta y)$$

  for $a \in \mathbf{F}_p$ and $\zeta \in \mu_{(p-1)d}$.
- Its de Rham H^1 has basis

$$\left\{ \omega_{i,j} = \frac{x^i y^j \mathrm{d}x}{y^{d-1}} \colon 0 \le i \le p-2,\ 0 \le j \le d-2 \right\}.$$

- If we restrict the action to the abelian subgroup $G = \mathbf{F}_p \times \mu_d$, H^1 decomposes into 1-dimensional eigenspaces for each character that is nontrivial on both $\mathbf{F}_p$ and μ_d.

The Hopkins-Mahowald affine group action. The Weierstrass equation for a general elliptic curve is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Under the affine coordinate change

$$x \mapsto x + r \qquad \text{and} \qquad y \mapsto y + sx + t$$

we get

$$\begin{aligned}
a_6 &\mapsto a_6 + a_4\,r + a_3\,t + a_2\,r^2 \\
&\qquad\qquad +a_1\,r\,t + t^2 - r^3 \\
a_4 &\mapsto a_4 + a_3\,s + 2\,a_2\,r \\
&\qquad\qquad +a_1(r\,s + t) + 2\,s\,t - 3\,r^2 \\
a_3 &\mapsto a_3 + a_1\,r + 2\,t \\
a_2 &\mapsto a_2 + a_1\,s - 3\,r + s^2 \\
a_1 &\mapsto a_1 + 2\,s.
\end{aligned}$$

This can be used to define an action of the affine group on the ring

$$A = \mathbf{Z}[a_1, a_2, a_3, a_4, a_6].$$

Its cohomology is the E_2-term of a spectral sequence converging to $\pi_*(\mathrm{tmf})$.

Theorem 2. *[Dieudonné] The category of formal groups over a finite field k is equivalent to the category of modules over the ring*

$$\mathbf{D}(k) = \mathbf{W}(k)\langle F, V\rangle/(FV = VF = p)$$

where $Fw = w^{\sigma}F$ and $Vw^{\sigma} = wV$ for $w \in \mathbf{W}(k)$. F is the Frobenius or pth power map, and V is the Verschiebung, the dual of F.

Examples:

- The Dieudonné module for the formal group law associated with the nth Morava K-theory is

  $$\mathbf{D}(\mathbf{F}_p)/(V - F^{n-1}),$$

  so in it we have $F^n = p$.
- More generally, for m and n relatively prime, let

  $$G_{m,n} = \mathbf{D}(k)/(V^m - F^n).$$

  It corresponds to an m-dimensional formal group of height $m + n$.

Theorem 3. *[Manin]*

(i) STRUCTURE THEOREM. *Any simple Dieudonné module M is isogenous over $\mathbf{W}(\overline{\mathbf{F}}_p)$ to some $G_{m,n}$.*

(ii) *Let the characteristic polynomial for F in M be*
$$Q(T) = T^m + \sum_{i>0} c_i T^{m-i}$$
for $c_i \in \mathbf{W}(k)$. If its Newton polygon has a line segment of horizontal length n and slope j/n, then up to isogeny over $\mathbf{W}(\overline{k})$, M has a summand of the form $G_{j,n-j}$.

The Newton polygon is the convex hull of the set of points
$$\{(i, \mathrm{ord}_p(c_i)) \colon 0 \le i \le m\},$$
where $c_0 = 1$. The condition on $Q(T)$ above is equivalent to the existence of n roots having p-adic valuation j/n.

Theorem 4. *[Manin, Tate, Honda]*

(i) RIEMANN SYMMETRY CONDITION. *If A is an abelian variety with formal completion $\widehat{A}$, and its Dieudonné module $D(\widehat{A})$ has a summand $G_{m,n}$ up to isogeny over $\mathbf{W}(\overline{\mathbf{F}}_p)$, then it also has a summand $G_{n,m}$.*

(ii) *More precisely, if A has dimension g and is defined over $\mathbf{F}_q$ with $q = p^a$, then the characteristic polynomial for F^a has the form*

$$Q_a(T) = T^{2g} + \sum_{0<i<2g} c_i T^{2g-i} + q^g$$

with $c_i \in \mathbf{Z}$, and

$$Q_a\left(\frac{q}{T}\right) = \frac{q^g Q_a(T)}{T^{2g}},$$

so $c_{g+i} = q^i c_{g-i}$ for $0 < i < g$. (The Newton polygon for $Q(T)$ is determined by that of $Q_a(T)$.)

(iii) CLASSIFICATION OF ABELIAN VARIETIES UP TO ISOGENY OVER $\mathbf{F}_q$. *There is a one-to-one correspondance between isogeny classes of abelian varieties over $\mathbf{F}_q$ and polynomials of the above form, all of whose roots have absolute value $\sqrt{q}$.*

Corollary 5.

(i) *For an elliptic curve* C*, either*

$$D(\widehat{C}) \cong G_{0,1} \oplus G_{1,0},$$

(the ordinary height 1 case) or

$$D(\widehat{C}) \cong G_{1,1},$$

(the supersingular height 2 case), up to isogeny over $\mathbf{W}(\overline{\mathbf{F}}_p)$*.*

(ii) *If an abelian variety* A *has a 1-dimensional formal summand of height* n *for* $n > 2$*, then the dimension of* A *is at least* n*.*

Theorem 6. *[Grothendieck, Berthelot] Let* C *be a smooth curve of genus* g *over* $\mathbf{F}_q$*. Then its crystalline (or de Rham)* H^1 *is a free* $\mathbf{W}(\mathbf{F}_q)$*-module of rank* $2g$ *isomorphic to the Dieudonné module of its Jacobian* $D(\widehat{J}(C))$*, with the induced action of the Frobenius* $\tilde{F}$ *relative to* $\mathbf{F}_q$ *coinciding with the action of* F^a*.*

THE WEIL CONJECTURES of 1949, proved by Deligne in 1974.

Given a smooth d-dimensional variety X over $\mathbf{F}_q$, its ZETA FUNCTION is defined by

$$Z(X,T) = \exp\left(\sum_{n>0} |X(\mathbf{F}_{q^n})| \frac{T^n}{n}\right).$$

Then

(i) $Z(X,T)$ is a rational function of T. (Proved by Dwork in 1960.)

(ii) More precisely,

$$Z(X,T) = \frac{P_1(T)P_3(T)\cdots P_{2d-1}(T)}{P_0(T)P_2(T)\cdots P_{2d}(T)}$$

where $P_i(T)$ is a polynomial whose degree is the rank of $H^i(X)$ suitably defined.

(iii) RIEMANN HYPOTHESIS IN CHARACTERISTIC p. Each reciprocal root of $P_i(T)$ has absolute value $q^{i/2}$.

(iv)

$$P_i(T) = \det(1 - T\tilde{F}|H^i(X))$$

where $\tilde{F}$ is the Frobenius relative to $\mathbf{F}_q$. Hence (ii) follows from an analog of the Lefschetz fixed point formula.

Weil proved these statements for curves. If X is a smooth curve of genus g, then

$$Z(X,T) = \frac{P_1(T)}{(1-T)(1-qT)},$$

where the factors $(1-T)^{-1}$ and $(1-qT)^{-1}$ correspond to H^0 and H^2. $P_1(T)$, which corrspsonds to H^1, has degree $2g$ with

$$P_1(T) = 1 + \sum_{0<i<2g} c_i T^i + q^g T^{2g},$$

and $Q_a(T) = T^{2g} P_1(1/T)$ is the characteristic polynomial of $\tilde{F} = F^a$ in $D(\widehat{J}(X))$. The coefficients c_i are the same as those in Theorem 4.

In other words, the zeta function of a curve determines the formal structure of its Jacobian in an explicit way.

Suppose X is acted on by a finite group G and let ρ be a representation of G over a suitable number field K. Define

$$L(X,\rho,T) = \exp\left(\frac{1}{|G|}\sum_{g\in G}\mathrm{Trace}(\rho(g))\sum_{n>0}C_n^g\frac{T^n}{n}\right),$$

where C_n^g is the number of points in x in $X(\overline{\mathbf{F}}_p)$ satisfying $g(x) = \tilde{F}^n(x)$.

When ρ is the regular representation, $L(X,\rho,T)$ is the zeta function. If the action of G is trivial and ρ is irreducible and nontrivial, then $L(X,\rho,T) = 1$.

We have

$$L(X,\rho_1\oplus\rho_2,T) = L(X,\rho_1,T)L(X,\rho_2,T)$$

so

$$Z(X,T) = \prod_{\rho \text{ irreducible}} L(X,\rho,T)^{\mathrm{degree}(\rho)}.$$

Deligne proved an alternating product formula for $L(X,\rho,T)$ similar to Weil's for $Z(X,T)$, in which $P_i^\rho(T)$ is the characteristic polynomial of $\tilde{F}$ restricted to

$$\mathrm{Hom}_G(\rho, H^i(X)\otimes_{\mathbf{W}(\mathbf{F}_q)} K).$$

Recall that our curve $C(p, f)$ admits an action of the abelian group

$$G = \mathbf{F}_p \times \mu_d \qquad \text{where } d = p^f - 1$$

that decomposes H^1 into 1-dimensional eigenspaces. It follows that

$$P_1(T) = \prod_{\chi} P_1^{\chi}(T),$$

where the product is over all characters χ that are nontrivial on both factors of G. Each of these factors of $P_1(T)$ is linear. They were computed in 1935 by Davenport and Hasse, who showed that the reciprocial roots of $P_1(T)$ (which are the roots of $Q_f(T)$) are certain Gauss sums, i.e., sums of pdth roots of unity. They can be computed explicitly for small values of p and f. The ideals that they generate, and hence their valuations with respect to a p-adic place in K, were determined by Stickelberger in 1890.

Theorem 7. *The characteristic polynomial* $Q(T)$ *for the Frobenius in the Dieudonné module* $D(\widehat{J}(C(p,f)))$ *has* $(p-1)b_i$ *roots with p-ordinal* $i/(p-1)$, *where*

$$\sum_i b_i t^i = \left(\frac{1-t^p}{1-t}\right)^f - 1 - t^{(p-1)f}$$

so for $0 < i < (p-1)f$,

$$b_i = \sum_{0 \le j \le i/p} (-1)^j \binom{f}{j} \binom{f+i-pj-1}{f-1},$$

e.g., $b_1 = f$.

Theorem 1 and more is a corollary of this.

Corollary 8. *In terms of Manin's structure theorem,*

$$D(\widehat{J}(C(p,1))) \cong \bigoplus_{0<i<p-1} G_{i,p-1-i}$$

$$D(\widehat{J}(C(p,2))) \cong \binom{p}{2} G_{1,1} \oplus \bigoplus_{0<i<p-1} \frac{i+1}{2}(G_{i,2p-2-i} \oplus G_{2p-2-i,i})$$

$$D(\widehat{J}(C(2,f))) \cong \bigoplus_{0<i<f} \binom{f}{i} \frac{1}{f} G_{i,f-i}$$

up to isogeny, where it is understood that $G_{km,kn} = kG_{m,n}$.

Here are some explicit values of the characteristic polynomial $Q(T)$ of the Frobenius (relative to $\mathbf{F}_p$) for the curve $C(p,f)$.

p	f	$Q(T)$
2	2	T^2+2
2	3	$T^6-2T^3+2^3$
2	4	$(T^8+2T^4+2^4)(T^2+2T+2)(T^2-2T+2)(T^2\pm 2)$
2	5	$T^{30}-6\,T^{25}-16\,T^{20}+352\,T^{15}-512\,T^{10}-6144\,T^5+32768$
2	6	$(T^{36}+6T^{30}+120T^{24}+384T^{18}+7680T^{12}+24576T^6+262144)$ $(T^{12}-12T^6+64)(T^{12}+12T^6+64)(T^2+2)^2$ $(T^2+2)\ (T^4-2\,T^2+4)\ (T^2+8)$
3	1	T^2+3
3	2	$(T^8-6T^4+81)(T^2-3)^2(T^2+3)$
3	3	$(T^{24}-87T^{18}+3321T^{12}-63423T^6+531441)$ $(T^{12}+9T^9+45T^6+243T^3+729)^2(T^2+3)$
5	1	$(T^8+30T^4+625)(T^2-5)^2$
5	2	$(T^2-5)^8\,(T^2+5)^4\,(T^8-30T^4+625)^2$ $(T^8+30T^4+625)\ (T^{16}+750T^4+390625)$ $(T^{32}+1380\,T^{24}+1103750\,T^{16}+539062500\,T^8+152587890625)$
7	1	$(T^{12}+4977T^6+117649)(T^6+7T^3+343)^2(T^2+7)^3$
11	1	$(672749994932560009201-14568299213068271\,T^{10}$ $+129620301481\,T^{20}-561671\,T^{30}+T^{40})$ $(25937424601-157668929\,T^5+467181\,T^{10}-979\,T^{15}+T^{20})^2$ $(T^2+11)^5$
13	1	$(542800770374370512771595361-415420467450868292270\,T^{12}$ $+126001160412387\,T^{24}-17830670\,T^{36}+T^{48})$ $(4826809+4381\,T^6+T^{12})^2(28561-130\,T^4+T^8)^3$ $(2197-65\,T^3+T^6)^4(-13+T^2)^6$

Isaac Newton Institute, Cambridge, UK