Handout on the Explicit Formula for Elliptic Curves

Steven Miller

October 23, 2001

1 The Explicit Formula

1.1 Summation Lemmas

We collect below certain basic integrals / sums that we will need.

Lemma 1.1 (Abel's Summation Formula - Integral Version) *Let $h(x)$ be a continuously differentiable function. Let $A(x) = \sum_{n \leq x} a_n$. Then*

$$\sum_{n \leq x} a_n h(n) = A(x)h(x) - \int_1^x A(u)h'(u)du \tag{1}$$

Lemma 1.2 (Partial Summation)

$$\sum_{M}^{N} a_n b_n = A_N b_N - A_{M-1} b_M + \sum_{M}^{N-1} A_n (b_n - b_{n+1}) \tag{2}$$

1.2 Preliminaries

Our studies will lead to investigating

$$\sum \phi(\gamma_E \frac{\log c_E}{2\pi}).$$

We first prove the explicit formula for $\sum \phi(\gamma_E)$, for replacing ϕ by ϕ_r, where $r = \frac{\log c_E}{2\pi}$, we obtain the desired formula. We record for later the relationship between $\hat{\phi}$ and $\hat{\phi}_r$, where $\hat{\phi}_r(\xi) = \hat{\phi}(r\xi)$.

Lemma 1.3 *Let $\hat{\phi}(\xi) = \int_{\mathbf{R}} \phi(x) e^{-2\pi i x \xi} dx$. Then $\hat{\phi}_r(\xi) = \frac{1}{r}\hat{\phi}(\xi/r)$.*

The proof is immediate from the definition of the Fourier Transform.

Lemma 1.4 (Sum of $\hat{\phi}$ over primes)

$$\frac{1}{\log N}\sum_{p\equiv 1(m)}\frac{\log p}{p}\hat{\phi}(a\frac{\log p}{\log N}) = \frac{1}{2a\phi(m)}\phi(0) + O(\frac{1}{\log N}). \tag{3}$$

Unfortunate notation, but denote the Euler Phi-function by φ. If m is a prime, $\varphi(m) = m-1$; in general, $\varphi(m)$ is the number of numbers from 1 to m that are relatively prime with m. We will use ϕ and $\hat{\phi}$ to denote a generic test function and its Fourier Transform. We will take ϕ to be an even Schwartz function, often with compact support.

By RH (or GRH if $m \neq 1$) and partial summation we have

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv 1(m)}} \log p &= \frac{x}{\varphi(m)} + O(x^{\frac{1}{2}}\log^2(mx)) \\ \sum_{\substack{p\le x\\ p\equiv 1(m)}} \frac{\log p}{p} &= \frac{\log x}{\varphi(m)} + O(1).\end{aligned} \tag{4}$$

For notational convenience, let $M = \varphi(m)$. Using partial summation on the p sum gives

$$\begin{aligned}\sum_{p\equiv 1(m)}\frac{\log p}{p}\hat{\phi}(a\frac{\log p}{\log N}) &= -\int_0^\infty \Big(\frac{\log x}{M} + O(1)\Big)\frac{d}{dx}\hat{\phi}(a\frac{\log x}{\log N}) \\ &= \int_0^\infty \frac{1}{Mx}\hat{\phi}(a\frac{\log x}{\log N}) + O\Big(\frac{1}{x\log N}\Big|\hat{\phi}(a\frac{\log x}{\log N})\Big|\Big) \\ &= \frac{\log N}{a}\int_0^\infty \frac{1}{M}\hat{\phi}(u) + O\Big(\frac{1}{\log N}\Big|\hat{\phi}(u)\Big|\Big)du \\ &= \frac{\log N}{a}\frac{1}{2}\int_{-\infty}^\infty \frac{1}{M}\hat{\phi}(u) + O\Big(\frac{1}{\log N}\Big|\hat{\phi}(u)\Big|\Big)du \\ &= \frac{\log N}{2aM}\phi(0) + O(1).\end{aligned} \tag{5}$$

Dividing by $\log N$ yields the lemma.

In particular, setting $m = 1$ and $a = 1, 2$ yields

Corollary 1.5 $\frac{1}{\log N}\sum_p \frac{\log p}{p}\hat{\phi}(\frac{\log p}{\log N}) = \frac{1}{2}\phi(0) + O(\frac{1}{\log N})$.

Corollary 1.6 $\frac{1}{\log N}\sum_p \frac{\log p}{p}\hat{\phi}(2\frac{\log p}{\log N}) = \frac{1}{4}\phi(0) + O(\frac{1}{\log N})$.

Let E be a modular elliptic curve (arising from a newform f on $\Gamma_0(N)$) whose zeros satisfy the GRH, namely $\rho_E = 1 + i\gamma_E$. To simplify notation, we drop the subscript E below. Then to E we can attach an L-function $L(s, E) = L(s)$. Define $\Lambda(s)$ by

$$\Lambda(s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(s).$$

Then we have

$$\Lambda(s) = \epsilon \Lambda(2 - s), \tag{6}$$

where $\epsilon = \epsilon_f = \pm 1$. The logarithmic derivative is

$$\frac{\Lambda'(s)}{\Lambda(s)} = \frac{1}{2} \log \frac{N}{4\pi^2} + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{L'(s)}{L(s)} = -\frac{\Lambda'(2-s)}{\Lambda(2-s)} \tag{7}$$

We express $\frac{L'(s)}{L(s)}$ in a form convenient for deriving the explicit formula. For each prime p, let E_p be the number of points on the reduced elliptic curve E (including infinity), and let $t_p = 1 + p - E_p$. Then it is well known (see, for example, AEC, page 240) that

$$L(s) = \prod_{p|\triangle} (1 - t_p p^{-s})^{-1} \prod_{p \ \dagger \ \triangle} (1 - t_p p^{-s} + p^{1-2s})^{-1} \tag{8}$$

$$L(s) = \sum \lambda(n) n^{-s}, \ \lambda(p) = t_p, \tag{9}$$

where if $p|\triangle$, then $t_p = -1, 0$, or 1. Hence we obtain

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle} \frac{d}{ds} \log(1 - t_p p^{-s}) - \sum_{p \ \dagger \ \triangle} \frac{d}{ds} \log(1 - t_p^{-s} + p^{1-2s}). \tag{10}$$

Straightforward calculations show the first term equals

$$-\sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{(\log p) t_p^k}{(p^k)^s}. \tag{11}$$

To handle the second term in the sum, we let $u = p^{-s}$ and factor

$$1 - t_p p^{-s} + p^{1-2s} = pu^2 - t_p u + 1 = (1 - \alpha_p u)(1 - \beta_p u), \tag{12}$$

where

$$\alpha_p + \beta_p = t_p, \quad \alpha_p \beta_p = p. \tag{13}$$

We see the second term in $\frac{L'(s)}{L(s)}$ is

$$\sum_{p \nmid \triangle} \sum_{k=1}^{\infty} \frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{14}$$

Combining yields

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{(\log p) t_p^k}{(p^k)^s} - \sum_{p \nmid \triangle} \sum_{k=1}^{\infty} \frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{15}$$

1.3 The Explicit Formula

The following derivation is a modification of that in Zeros of Principle L-Functions (Rudnick and Sarnak, Duke Journal of Mathematics, 1996). See their proposition 2.1, pages 277-278.

Let $\phi \in \mathcal{S}(\mathbf{R})$ be an even function whose Fourier Transform has compact support. By the GRH, the non-trivial zeros of the L-function associated to our elliptic curve satisfy

$$\rho = 1 + i\gamma, \quad \gamma \in \mathbf{R}.$$

Note that for $Re(s) = 1$, $\frac{s-1}{i} \in \mathbf{R}$, and hence $\phi(\frac{s-1}{i})$ exists and is well defined. We are thus led to define

$$H(s) = \phi(\frac{s-1}{i}). \tag{16}$$

Initially, $H(s)$ is defined only for $Re(s) = 1$. Using the Inverse Fourier Transform we see

$$\phi(x) = \int_{\mathbf{R}} \hat{\phi}(\xi) e^{2\pi i x \xi} d\xi. \tag{17}$$

Therefore

$$\phi(x+iy) = \int_{\mathbf{R}} \hat{\phi}(\xi) e^{2\pi i (x+iy)\xi} d\xi, \tag{18}$$

and as ϕ has compact support, we see we can extend ϕ, and hence $H(s)$ is well defined, and

$$H(x+iy) = \int_{\mathbf{R}} \left[\hat{\phi}(\xi) e^{2\pi(x-1)\xi} \right] e^{2\pi i y \xi} d\xi. \tag{19}$$

Thus $H(x+iy)$ is the Fourier Transform of a function in $\mathcal{S}(\mathbf{R})$, and hence is rapidly decreasing in $Im(s) = y$.

So both $H(s)$ and $\Lambda(s)$ are nice entire functions. Consider

$$\mathcal{I} = \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s) ds. \tag{20}$$

We shift contours from $Re(s) = 2\frac{1}{2}$ to $-\frac{1}{2}$. This picks up zeros/poles of $\Lambda(s)$. Two factors of $\Lambda(s)$ contribute potential zeros/poles, the L term and the Γ term. The only pole of the Γ-function in this range is at $s = 0$; however, as $\Lambda(2) \neq 0$, there is a zero of the L-function that cancels. Hence the only surviving zeros/poles are from the zeros of the L function in the critical strip, and the residue is just $H(1+i\gamma) = \phi(\gamma)$. Therefore

$$\mathcal{I} = \sum \phi(\gamma) + \frac{1}{2\pi i} \int_{Re(s)=-\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s) ds. \tag{21}$$

By (7), we have $\frac{\Lambda'(s)}{\Lambda(s)} = -\frac{\Lambda'(2-s)}{\Lambda(2-s)}$, so substituting this above and changing s to $2-s$ we obtain

$$\mathcal{I} = \sum \phi(\gamma) - \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(2-s) ds. \tag{22}$$

Bringing $\sum \phi(\gamma)$ over to the LHS and recalling the definition of $\mathcal{I}$ yields

$$\sum \phi(\gamma) = \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} \Big[H(s) + H(2-s) \Big] ds. \tag{23}$$

We can shift the contour above to $Re(s) = 1$, as we are assuming there are no zeros of the L-function off the critical line. We do so, and note that for $s = 1+iy$, $H(2-s) = H(s) = \phi(y)$, as we are assuming ϕ even. Using (7) for $\frac{\Lambda'(s)}{\Lambda(s)}$ gives (for $s = 1+iy, ds = idy$)

$$\begin{aligned} \sum \phi(\gamma) &= \frac{1}{2\pi} \int_{\mathbf{R}} \left[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)} \right] \phi(y) dy \\ &+ \frac{1}{2\pi i} \int_{\mathbf{R}} \frac{L'(1+iy)}{L(1+iy)} 2\phi(y) ds. \end{aligned} \tag{24}$$

We use (15) to substitute for $\frac{L'(1+iy)}{L(1+iy)}$; by Hasse's theorem $|t_p| < 2p^{\frac{1}{2}}$. We shift this piece back to $Re(s) = 2\frac{1}{2}$. By the DCT we can interchange the summations and integration. We then shift back to $Re(s) = 1$. As

$$\int_{\mathbf{R}} (\frac{1}{p^k})^{1+iy}\phi(y)dy = \int_{\mathbf{R}} \frac{1}{p^k}\phi(y)e^{-ik\log(p)y}dy = \frac{1}{p^k}\hat{\phi}(\frac{k\log(p)}{2\pi}), \tag{25}$$

we obtain the explicit formula:

$$\begin{aligned}\sum \phi(\gamma) &= \frac{1}{2\pi}\int_{\mathbf{R}} \left[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\right]\phi(y)dy \\ &- \frac{1}{2\pi}\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{2\log(p)t_p^k}{p^k}\hat{\phi}(\frac{1}{2\pi}k\log(p)) \\ &- \frac{1}{2\pi}\sum_{p\ \dagger\ \triangle}\sum_{k=1}^{\infty}\frac{2\log(p)(\alpha_p^k+\beta_p^k)}{p^k}\hat{\phi}(\frac{1}{2\pi}k\log(p))\end{aligned} \tag{26}$$

1.4 Tractable Explicit Formula

In the previous section, we derived the explicit formula for the sum over the zeros of an elliptic curve (assuming the GRH, of course). Below we will show that many of the terms are $O(\frac{1}{\log N})$.

First, we replace $\phi(x)$ by $\phi_r(x)$, $r = \frac{1}{2\pi}\log N$. A straightforward calculation shows that

$$\frac{1}{2\pi}\int_{\mathbf{R}}\left[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\right]\phi(y)dy \to \int_{\mathbf{R}}\phi(y)dy + O(\frac{1}{\log N}). \tag{27}$$

To prove the above, use (see Alfohrs, Complex Analysis)

$$\frac{\Gamma'(z)}{\Gamma(z)} = C + \log z - \frac{1}{2z} - \int_0^{\infty}\frac{2u}{u^2+z^2}\frac{du}{e^{2\pi u}-1},\ Re(z) > 0. \tag{28}$$

Hence we find

$$\begin{aligned}\sum \phi(\gamma\frac{\log N}{2\pi}) &= \int_{\mathbf{R}}\phi(y)dy \\ &- 2\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{\log p}{\log N}\frac{t_p^k}{p^k}\hat{\phi}(k\frac{\log p}{\log N}) \\ &- 2\sum_{p\ \dagger\ \triangle}\sum_{k=1}^{\infty}\frac{\log p}{\log N}\frac{\alpha_p^k+\beta_p^k}{p^k}\hat{\phi}(k\frac{\log p}{\log N}) + O(\frac{1}{\log N}).\end{aligned} \tag{29}$$

As $|\alpha_p|, |\beta_p| < p^{\frac{1}{2}}$ and $|t_p| \leq 2p^{\frac{1}{2}}$, we can bound the $k \geq 3$ terms above by $||\phi||_\infty \frac{1}{\log N}$. For $p \dagger \triangle$, $\alpha_p + \beta_p = t_p$ and $\alpha_p \beta_p = p$. Hence $\alpha_p^2 + \beta_p^2 = t_p^2 - 2p$, and it is sufficient to study

$$\begin{aligned}
\sum \phi(\gamma \frac{\log N}{2\pi}) &= \int_{\mathbf{R}} \phi(y) dy \\
&- 2 \sum_p \sum_{k=1}^{2} \frac{\log p}{\log N} \frac{t_p^k}{p^k} \hat{\phi}(k \frac{\log p}{\log N}) \\
&- 2 \sum_{p \dagger \triangle} \frac{\log p}{\log N} \frac{-2p}{p^2} \hat{\phi}(2 \frac{\log p}{\log N}) + O(\frac{1}{\log N}). \qquad (30)
\end{aligned}$$

Lemma 1.7 $\frac{1}{\log N} \sum_{p|\triangle} \frac{\log p}{p} \hat{\phi}(a \frac{\log p}{\log N}) = O(\frac{\log \log N}{\log N})$.

In the above, $\triangle$ is the discriminant of the elliptic curve, and N is its conductor. Further, the conductor and the discriminant have the same prime factors, so we may replace $\triangle$ by N.

$\frac{\log p}{p}$ is a decreasing function, so in the sum, the sum is largest when we have many small prime factors of N; in fact, the sum is greatest when N is the product of the first n primes. So

$$N = 2 \cdot 3 \cdots p_n \geq 2^n \rightarrow n \leq \frac{\log N}{\log 2}. \qquad (31)$$

As $\sum_{p=2}^{X} \frac{\log p}{p} = \log X + O(1)$ (Davenport, Multiplicative Number Theory, page 57) we have

$$\begin{aligned}
\frac{1}{\log N} \sum_{p|N} \frac{\log p}{p} \hat{\phi}(a \frac{\log p}{\log N}) &\ll \frac{1}{\log N} \sum_{p=2}^{\frac{\log N}{a \log 2}} \frac{\log p}{p} \\
&= \frac{1}{\log N} \left[\log(\frac{\log N}{a \log 2}) + O(1) \right] \\
&= O(\frac{\log \log N}{\log N}), \qquad (32)
\end{aligned}$$

yielding the lemma.

Therefore, the cost of expanding $\sum_{p \dagger \triangle} \frac{\log p}{\log N} \frac{-2p}{p^2} \hat{\phi}(2 \frac{\log p}{\log N})$ to a sum over all primes can be safely absorbed in our error. Therefore we now study

$$\sum \phi(\gamma \frac{\log N}{2\pi}) = \int_{\mathbf{R}} \phi(y)dy - 2\sum_p \sum_{k=1}^{2} \frac{\log p}{\log N} \frac{t_p^k}{p^k} \hat{\phi}(k \frac{\log p}{\log N}) - 2\sum_p \frac{\log p}{\log N} \frac{-2p}{p^2} \hat{\phi}(2\frac{\log p}{\log N}) + O(\frac{1}{\log N}). \quad (33)$$

The last sum, by Lemma 1.4, is just $4\frac{1}{4}\phi(0) = \phi(0)$. Thus we can write the explicit formula as:

$$\sum \phi(\gamma \frac{\log N}{2\pi}) = \int_{\mathbf{R}} \phi(y)dy + \phi(0) - 2\sum_p \frac{\log p}{\log N} \frac{t_p}{p} \hat{\phi}(\frac{\log p}{\log N}) - 2\sum_p \frac{\log p}{\log N} \frac{t_p^2}{p^2} \hat{\phi}(2\frac{\log p}{\log N}) + O(\frac{\log \log N}{\log N}). \quad (34)$$

We make one final simplification. $t_p = 1 + p - E_p$, where E_p is the number of points (including infinity) on the curve reduced mod p. Let us say $y^2 = f(x)$. Then $E_p = 1 + \sum_{x=0}^{p-1} \left(1 + (\frac{f(x)}{p})\right)$. Hence $t_p = -\sum_{x=0}^{p-1} (\frac{f(x)}{p})$, and we have

Theorem 1.8 (The Explicit Formula)

$$\begin{aligned}
\sum \phi(\gamma \frac{\log N}{2\pi}) &= \int_{\mathbf{R}} \phi(y)dy + \phi(0) \\
&- 2\sum_p \frac{\log p}{\log N} \frac{t_p}{p} \hat{\phi}(\frac{\log p}{\log N}) \\
&- 2\sum_p \frac{\log p}{\log N} \frac{t_p^2}{p^2} \hat{\phi}(2\frac{\log p}{\log N}) + O(\frac{\log \log N}{\log N}) \\
&= \int_{\mathbf{R}} \phi(y)dy + \phi(0) \\
&+ 2\sum_p \frac{\log p}{\log N} \frac{1}{p} \hat{\phi}(\frac{\log p}{\log N}) \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) \\
&- 2\sum_p \frac{\log p}{\log N} \frac{1}{p^2} \hat{\phi}(2\frac{\log p}{\log N}) \Big(\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)\Big)^2 + O(\frac{\log \log N}{\log N})
\end{aligned} \quad (35)$$