Math 581g, Fall 2011, Homework 6: SOLUTIONS

William Stein (wstein@uw.edu)

December 1, 2011

1. **(Warm up)** Using the formula from class (or the book), compute the genus of the modular curve $X(54)$. Be prepared: what is the genus of $X(2012)$?

   Solution. The formula for the genus of $X(N)$ (for $N \geq 3$) is $g = 1 + \frac{d}{12N}(N-6)$, where $d = \#\,\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})/2 = N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right)$. Here is an implementation in Sage:

```
def genus(N):
    d = N^3*prod(1-1/p^2 for p in N.prime_divisors())/2
    return 1+d*(N-6)/(12*N)
```

   And here we use it to solve the problem:

```
sage: genus(3) # double check
0
sage: genus(5) # double check
0
sage: genus(7) # double check
3
sage: genus(54)
3889
sage: genus(2012)
253767025
```

2. Consider the map $j : X(N) \to \mathbf{P}^1_{\mathbf{C}}$ for $N \geq 3$. Following the argument presented in class, prove that
$$\#j^{-1}(1728) = \frac{\#\,\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})}{4}.$$

   Solution. Let $\tau = i$, so $j(\tau) = 1728$. The automorphism group of $E_\tau = \mathbf{Z}i + \mathbf{Z}$ is of order 4, generated by the automorphism $[i]$ induced by multiplication by $i \in \mathrm{End}(E_\tau)$. We have $P_\tau = 1/N$ and $Q_\tau = i/N$, which have Weil pairing -1. With respect to the basis P_τ, Q_τ, the matrix of $[i]$ is $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. The powers of A are:
$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

   Since $\det(A) = 1$, and the above 4 matrices are distinct modulo $N \geq 3$, we see that the set of triples (E, P, Q) with $j(E) = 1728$ are divided up into orbits of size 4 by $[i]$, as claimed.

3. Explicitly compute the sets $\Gamma_0(N)\backslash\mathbf{P}^1(\mathbf{Q})$ for $N = 3$, $N = 9$, and $N = 54$, using the method I described in class. [**Hint: You should double check your work with Sage:** `Gamma0(N).cusps()`**, but don't just get the answer this way.**]

   Solution. This problem is pretty tedious to solve by hand. The answer you should get is as follows:

```
sage: Gamma0(3).cusps()
[0, Infinity]
sage: Gamma0(9).cusps()
[0, 1/3, 2/3, Infinity]
sage: Gamma0(54).cusps()
[0, 1/27, 1/18, 1/9, 1/6, 2/9, 5/18, 1/3, 1/2, 2/3, 5/6, Infinity]
```

4. Let N be a positive integer. Prove that

$$\#\,\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) = N^3 \cdot \prod_{p\mid N} \left(1 - \frac{1}{p^2}\right),$$

where the product is over the prime divisors of N.

Solution. First reduce to the prime power case, by noting that $\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z}) \cong \prod_{p\mid N} \mathrm{SL}_2(\mathbf{Z}/p^{\nu_p}\mathbf{Z})$. Next, compute the cardinality of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ using the exact sequence

$$1 \to K \to \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \to 1,$$

where K is by definition the kernel, which has a simple description as

$$K = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + A \,:\, A \in pM_{2\times 2}(\mathbf{Z}/p^n\mathbf{Z}) \right\}.$$

We find that

$$\begin{aligned}\#\,\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) &= \#\,\mathrm{GL}_2(\mathbf{Z}/p\mathbf{Z}) \cdot \#K \\ &= ((p^2-1)\cdot(p^2-p))\cdot p^{4(n-1)}\end{aligned}$$

Using the exact sequence

$$1 \to \mathrm{SL}_2(\mathbf{Z}/p^n\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z}) \to (\mathbf{Z}/p^n\mathbf{Z})^* \to 1$$

we relate the cardinality of $\mathrm{SL}_2(\mathbf{Z}/p^n\mathbf{Z})$ to that of $\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})$ to obtain

$$\begin{aligned}\#\,\mathrm{SL}_2(\mathbf{Z}/p^n\mathbf{Z}) &= \frac{\#\,\mathrm{GL}_2(\mathbf{Z}/p^n\mathbf{Z})}{\#(\mathbf{Z}/p^n\mathbf{Z})^*} \\ &= \frac{(p^2-1)\cdot(p^2-p)\cdot p^{4(n-1)}}{p^{n-1}(p-1)} \\ &= \frac{(p-1)^2\cdot(p+1)\cdot p^{4(n-1)+1}}{p^{n-1}(p-1)} \\ &= p^{3n}p^{-2}(p-1)(p+1) = N^3\left(1-\frac{1}{p^2}\right).\end{aligned}$$