Good Primes for Supersingular $2, 3$-Isogeny Graphs

Sarah Arpin
Graduate Student at the University of Colorado Boulder
Sarah.Arpin@colorado.edu

Abstract

In this note, we investigate the congruence conditions on p which leave us with no loops and no multi-edges in the supersingular elliptic curve 2-isogeny graph and the supersingular elliptic curve 3-isogeny graph. We put these conditions together to get primes p for which the 2,3-isogeny graph will have neither loops nor multi-edges (with the same edge label - a pair of vertices connected by a 3-isogeny and a 2-isogeny edge is still allowed). Unfortunately, these conditions are incompatible with the protocols for SIKE [Jao] and CSIDH [CLM+18], which use $p = 2^{k_1}3^{k_2} - 1$ for large k_1, k_2. Under these constraints, we make additional recommendations to minimize the number of loops and multi-edges in graphs used for these protocols.

1 How to guarantee no loops, no multi-edges 2-isogeny graph

In this section, we discuss the condition necessary on p in order for the supersingular elliptic curve 2-isogeny graph over $\overline{\mathbb{F}}_p$ to be free of loops and multi-edges.

1.1 Loops

Loops happen when there are supersingular roots to $\Phi_2(X, X)$:

$$\Phi_2(X, X) = -(X + 3375)^2(X - 1728)(X - 8000)$$

- $X + 3375$ is the Hilbert Class Polynomial of $\mathbb{Q}(\sqrt{-7})$. This j-invariant will be supersingular if and only if p is inert in $\mathbb{Q}(\sqrt{-7})$. Doing Legendre symbol calculations, we see that $j = -3375$ will *not* be supersingular for $p \equiv 1, 2, 4 \pmod 7$.
- $j = 1728$ is *not* supersingular precisely for $p \equiv 1 \pmod 4$ (a classical fact from [Sil09], for example).
- $X - 8000$ is the Hilbert Class Polynomial of $\mathbb{Q}(\sqrt{-2})$. $j = 8000$ is *not* supersingular for $p \equiv 1, 3 \mod 8$.

Taking these conditions together, we get $p \equiv 1 \pmod 8$ and $p \equiv 1, 2, 4 \pmod 7$. Solving this system of congruences, we get the condition

$$p \equiv 1, 9, 25 \pmod{56}$$

to guarantee $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ has no loops.

1.2 Multi-edges

Multi-edges happen when the resultant of $\Phi_2(X, Y)$ and $\frac{d}{dY}\Phi_2(X, Y)$ in Y has roots which give supersingular j-invariants. Calculating this resultant in Sage ([The19]) gives:

$$-4(X + 3375)^2(X - 1728)X^2(X^2 + 191025X - 121287375)^2.$$

- Discussed above, $j = -3375$ is *not* supersingular for $p \equiv 1, 2, 4 \pmod 7$.
- $j = 1728$ is *not* supersingular for $p \equiv 1 \pmod 4$.
- $j = 0$ is *not* supersingular for $p \equiv 1 \pmod 3$.
- $X^2 + 191025X - 121287375$ is the Hilbert Class Polynomial of $\mathbb{Q}(\sqrt{-15})$. It is supersingular whenever p is not inert in $\mathbb{Q}(\sqrt{-15})$, or whenever $\left(\frac{-15}{p}\right) = 1$ (for $p > 5$). Taking into consideration the conditions $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$ above, this happens precisely when $p \equiv 1, 4 \pmod 5$.

Putting these conditions together, we see that $\mathcal{G}_2(\overline{\mathbb{F}}_p)$ is multi-edge-free for p satisfying:

$$p \equiv 1, 121, 361, 169, 289, 109 \pmod{420}$$

1.3 No Loops, No Multi-edges

Putting together the stipulations of the previous two sections, the following congruence classes of primes p will have neither loops nor multi-edges in the supersingular 2-isogeny graph:

$$p \equiv 1, 121, 361, 169, 289, 109 \pmod{840}.$$

2 How to guarantee no loops, no multi-edges 3-isogeny graph

2.1 Loops

$\Phi_3(X, X)$ factors:

$$-(X - 8000)^2(X - 54000)X(X + 32768)^2$$

- $j = 8000$ is *not* supersingular for $p \equiv 1, 3 \pmod 8$.
- $j = 54000$ is always 2-isogenous to $j = 0$, so these two lie on the same component of the ℓ-isogeny graph, for any ℓ. $j = 54000$ will be supersingular precisely when $j = 0$ is supersingular. In particular $j = 54000$ and $j = 0$ are *not* supersingular for $p \equiv 1 \pmod 3$.
- $X + 32768$ is the Hilbert Class Polynomial of $\mathbb{Q}(\sqrt{-11})$. $j = -32768$ will be supersingular whenever p is not inert in $\mathbb{Q}(\sqrt{-11})$. Assuming $p > 11$ and $p \equiv 1, 3 \pmod 8$, a Legendre symbol calculation gives the following condition on p for $j = -32768$ to *not* be supersingular:

$$p \equiv 1, 3, 4, 5, 9 \pmod{11}$$

Putting these congruence conditions together, we see that $\mathcal{G}_3(\overline{\mathbb{F}}_p)$ is loop-free for p satisfying:

$$p \equiv 1, 25, 49, 67, 91, 97, 115, 163, 169, 235 \pmod{264}$$

2.2 Multi-edges

As in the 2-isogeny multi-edge case, we consider the roots of the resultant of $\Phi_3(X, Y)$ and $\frac{d}{dY}\Phi_3(X, Y)$ in Y. Calculating and factoring this resultant gives:

$$-27(X^2 - 52250000X + 12167000000)^2(X - 8000)^2(X^2 + 117964800X - 134217728000)^2$$

$$(X^2 - 1264000X - 681472000)^2(X + 32768)^2(X - 1728)^2X^2$$

- $j = 1728$ is *not* supersingular for $p \equiv 1 \pmod 4$.
- The roots of $X^2 - 52250000X + 12167000000$ are 2-isogenous to $j = 8000$. In particular, these are on the same component of the ℓ-isogeny graph for any ℓ. The roots of this polynomial and $j = 8000$ are *not* be supersingular for $p \equiv 1, 3 \pmod 8$.
  Since we also have $p \equiv 1 \pmod 4$, this leaves $p \equiv 1 \bmod 8$.
- $X^2 - 1264000X - 681472000$ is the Hilbert Class polynomial of $\mathbb{Q}(\sqrt{-5})$. Taking into account we already have $p \equiv 1 \pmod 8$, looking for where p is split in $\mathbb{Q}(\sqrt{-5})$ is equivalent to finding when $\left(\frac{-5}{p}\right) = 1$. Under the assumption $p \equiv 1 \pmod 8$, $\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = 1$. This gives the condition $p \equiv 1, 4 \bmod 5$.
- $X^2 + 117964800X - 134217728000$ is the Hilbert Class polynomial of $\mathbb{Q}(\sqrt{-35})$. Takine into account we already require $p \equiv 1 \pmod 8$ and $\left(\frac{5}{p}\right) = 1$, we get the additional congruence condition:

$$p \equiv 1, 2, 4 \pmod 7.$$

- As seen above $j = -32768$ is *not* supersingular for $p \equiv 1, 3, 4, 5, 9 \pmod{11}$.

- $j = 0$ is *not* supersingular for $p \equiv 1 \pmod 3$.

Putting these all together an eliminating redundancies, we get the system of linear congruences:

$$p \equiv 1, 3, 4, 5, 9 \pmod{11}$$

$$p \equiv 1 \pmod 3$$

$$p \equiv 1 \pmod 8$$

$$p \equiv 1, 4 \pmod 5$$

$$p \equiv 1, 2, 4 \pmod 7.$$

Solving this system gives:

$$p \equiv 1, 169, 289, 361, 529, 841, 961, 1369, 1681, 1849, 2209, 2641, 2689, 2809,$$

$$3481, 3529, 3721, 4321, 4489, 5041, 5329, 5569, 6169, 6241, 6889, 7561, 7681, 7921, 8089, 8761 \pmod{9240}.$$

2.3 No Loops, No Multi-edges

Notice that the condition of "no multi-edges" also encompasses the condition of "no loops", so p's for which $\mathcal{G}_3(\overline{\mathbb{F}}_p)$ is free of loops and multi-edges are:

$$p \equiv 1, 169, 289, 361, 529, 841, 961, 1369, 1681, 1849, 2209, 2641, 2689, 2809,$$

$$3481, 3529, 3721, 4321, 4489, 5041, 5329, 5569, 6169, 6241, 6889, 7561, 7681, 7921, 8089, 8761 \pmod{9240}.$$

3 2,3-Isogeny Graph

Putting together the recommendations of the previous section, to guarantee that the supersingular 2,3-isogeny graph is free of loops and multi-edges (multi-edges of the same degree isogeny), we require:

$$p \equiv 1, 169, 289, 361, 841, 961, 1681, 1849, 2641, 2689, 2809,$$

$$3481, 3529, 3721, 4321, 4489, 5041, 5329, 6169, 6241, 6889, 7561, 7681, 7921, 8761 \pmod{9240}$$

4 Realistic Recommendations for p

The recommendations of the previous two sections would indicate that, if you wanted a supersingular $2, 3$-isogeny graph with no multiple edges and no loops, you would want:

$$p \equiv 1, 169, 289, 361, 841, 961, 1681, 1849, 2641, 2689, 2809,$$

$$3481, 3529, 3721, 4321, 4489, 5041, 5329, 6169, 6241, 6889, 7561, 7681, 7921, 8761 \pmod{9240}$$

However, current protocols rely on primes being of the form $2^{k_1}3^{k_2} - 1$, with large k_1, k_2. This essential forces $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$. Recomputing congruence conditions to *minimize* the number of loops and multi-edges in the $2, 3$-isogeny graphs (i.e., only changing the congruence conditions modulo 3 and 4 in the calculations above), we recommend:

$$p \equiv 23, 323, 443, 683, 863, 947, 1103, 1247, 1367, 1523, 1607, 1703, 1787,$$

$$2003, 2027, 2363, 2423, 2447, 2627, 2843, 2927, 2963, 3287, 3347, 3623,$$

$$3683, 3767, 3887, 4547, 4607 \pmod{4620}.$$

References

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018. `https://eprint.iacr.org/2018/383`.

[Jao] David Jao. SIKE. `http://sike.org`. Accessed: 2019-11-13.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves, 2nd Edition.* Springer-Verlag, New York, N.Y., 2009.

[The19] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7)*, 2019. `https://www.sagemath.org`.