Chalkboard #12

Elliptic Curves over the rational number field

This chalkboard should have been an appendix to Chalkboard #3 on Classification of Prime Numbers. I previously defined three types of primes which were used to classify the period length of the Perrin sequence modulo (p).

If we start to look for rational solutions mod (p) to the elliptic curve defining the Perrin sequence the reason for this classification becomes apparent.

The ideas for this chalkboard came after reading "Fearless Symmetry" by Avner Ash and Robert Gross (Princeton University Press) 2006.

Given two polynomials:

$$f(y) := y^2$$

$$f(x) := x^3 + A \cdot x + B$$

Find all integers greater or equal to zero that satisfy

f(y) = f(x)

There is an amazing "conjecture" ,the Birch Swinnerton Dyer Conjecture that predicts how many rational points are solutions modulo q for a given elliptic curve.

To paraphrase Ash and Gross (pg 207)

Theorem 18.5 Let q be a prime other that a prime p that is unramified for the Galois representation ψ. (This is true if q does not divide the discriminant $2p(4A^2+27B^2)$). The matrix $\psi(Frob_q)$ is only defined up to conjugacy, but (the character) $\chi_\psi(Fob_q)$ is well defined and

$\chi_\psi(Frob_q) = 1 + q - \#E(F_q)$

Here $\#E(F_q)$ means the number of points in $E(F_q)$. In other words $\#E(F_q)$ equals the number of solutions to the congruence $y^2 = x^3 + Ax + B \pmod q$ defining the elliptic curve E, plus 1 for O, the point at infinity.

The linear representation of an elliptic equation is given by the matrix of Frobenius elements ψ**(Frob$_q$)** which are elements of the Galois group representing the action of **Frob$_q$** on the algebraic integers. The Frobenius character χ_ψ**(Frob$_q$)** is formed from the trace of this matrix which is defined for each conjugacy class.

Fortunately for elliptic curves, the Frobenius character is a real integer even though elements of the Galois group can be complex numbers. This can be seen from the integer equation defined above which relates χ_ψ**(Frob$_q$)** to **#E(F$_q$).**

As seen below, **Frob$_q$** also determines the cycle type of a degree 3 polynomial. There are three cycle types:

1. The elliptic curve E factors into three linear factors modulo q
2. The elliptic curve E factors into one linear and one quadratic factor modulo q.
3. There is no factorization of the elliptic curve modulo q

Later in their book the 'cuspidal normalized newform' is explained:

Let

$$q := \exp(2\cdot\pi\cdot i\cdot\tau)$$

And the modular sequence (newform)

$$S(q) := q + a_2\cdot q^2 + a_3\cdot q^3 + ..$$

Then there exists
(Theorem 21.1)

1. a positive integer N called the level (conductor) of the newform
2. a field k that contains Q$_p$ and all the coefficients a$_i$
3. A two dimensional linear Galois representation
τ:G --→ GL((2,k):

which obey the rule: If p is any prime that does not evenly divide N then τ is unramified at p and
χ_τ(Frob$_p$) = a$_p$.

.

There is an abstract connection between a_p and $\chi_\tau(Frob_p)$!!

Fortunately the application of these relations is simple and can be used to explain a connection between the period length of a sequence (mod(p)) (Chalkboard #2), the type of prime p (Chalkboard #3) and the number of integer solutions given by the modular (newform) S(q)

Look at p= 5 mod(5)

the equation $y^2 = x^3-x-1$ has 8 integer solutions including infinity

(0,2), (0,3) (1,2) (1,3) (2,0) (4,2) (4,3) and infinity O

reduce mod 5

Based on the theorems above

$\chi_\tau(Frob_5) = a_5$

$\chi_\psi(Frob_5) = 1 + 5 - \#E(F_5) = 6- 8 = -2$

or $a_5 = -2$

This requires that 5 is not a divisor of the level (conductor) of E(Q). For the equation $y^2 = x^3-x-1$ the discriminant equals the conductor and is $368 = 4^2*23$ so all primes except 23 and powers of 2. These numbers are "ramified" and considered "bad primes" so are excluded from the Frobenius representation.

Look at p= 13 mod(13)

the equation $y^2 = x^3-x-1$ has 19 integer solutions including infinity

(0,5),(0,8),(1,5),(1,8),(3,6),(3,7),(6,10),(6,12),(7,6),(7,7),(8,10),(8,3),(9,2),(9,11),(10,1), (10,12),(12,5),(12,8) and infinity O

reduce mod 13

Based on the theorems above

$\chi_\tau(\text{Frob}_{13}) = a_{13}$

$\chi_\psi(\text{Frob}_{13}) = 1 + 13 - \#E(F_{13}) = 14 - 19 = -5$

or $a_{13} = -5$

The modular form then looks something like:

$S(q) = q + 3q^3 - 2q^5 + 4q^7 + 6q^9 - 2q^{11} - 5q^{13} + ..$

Note: The first 100 terms for a_p can be found at the website **Lmfdb.org**. Search under Conductor = 368 which is the same as the discriminant for the equation $y^2 = x^3 - x - 1$

All equations of the Weierstrass form $y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6$ can be represented as

$(A_1, A_2, A_3, A_4, A_6)$ Our equation is then (0,0,0,-1,-1)

This form will be used to define other equations below

Now for some interesting observations:

1. Note that for p =5 there is a solution (2,0) for $y^2 = 0$
2. Note that for p = 13 there is no solution for y = 0
3. If the first 100 values of a_p are reviewed then it is observed that for all type 1 primes a_p are even, for type 2 primes a_p are odd and for type 3 primes a_p is either even or odd.
4. If the first 100 values of a_p are reviewed then observation 1 and observation 2 hold for type 1 and type 2 primes.

Discussion of the least period for irreducible characteristic polynomials

As discussed above the character χ_τ**(Frob$_q$)**

indicates how the polynomial $x^t - 1$ factors over the field of integers F_q.

The "order" of a polynomial f(x) with f(0) not zero, is the smallest integer t for which f(x) divides the polynomial mod q

Theorem from Lidl, R, and Niederreiter "Introduction to Finite Fields and their Application" Cambridge University Press) 1994.(pg 204)

Let f(x) Ξ F_q(x) be an irreducible polynomial over F_q with degree(f(x))=k. Then ord(f(x)) divides q^k -1.

This theorem is the key to defining type 1, type 2 and type 3 primes in Chalkboard #3.

Conjecture:
1. Let p be a type 1 prime. (prime which is not a square mod 23) Then the equation
f(x) = x^3 -x-1 mod p factors into one linear (degree 1) and one quadratic (degree 2) equations

2. Let p be a type 2 prime. (prime which is a square mod 23) Then the equation
f(x) = x^3 -x-1 mod p does not factor.

3. Let p be a type 3 prime.(prime factors two terms $a^2 + 23\ b^2$) Then the equation
f(x) = x^3 -x-1 mod p factors into three linear equations

Example: Type 1 prime p = 17

$\mathrm{mod}\left[\left(y_i\right)^2, 17\right]$

0
1
4
9
16
8
2
15
13
13
15
2
8
16
9
4

$\mathrm{mod}\left[\left(x_i\right)^3 - x_i - 1, 17\right]$

-1
-1
5
6
8
0
5
12
10
5
3
10
15
7
9
10

$$f17(x) := (x-5)\cdot\left(x^2 + 5\cdot x + 7\right)$$

$$s171 := \frac{-5+\sqrt{-3}}{2} \qquad f17(s171) = 0$$

$$s172 := \frac{-5-\sqrt{-3}}{2} \qquad f17(s172) = 0$$

Type 2 prime p =13

$\mathrm{mod}\left[\left(y_i\right)^2, 13\right]$

0
1
4
9
3
12
10
10
12
3
9
4
1
0
1
4

$\mathrm{mod}\left[\left(x_i\right)^3 - x_i - 1, 13\right]$

-1
-1
5
10
7
2
1
10
9
4
1
6
12
12
12
5

Note that for type 2 primes there is no solution for y = 0 so the equation x^3 -x-1 is irreducible

Type 3 prime p =23

$\mathrm{mod}\left[\left(y_i\right)^2, 23\right]$

0
1
4
9
16
2
13
3
18
12
8
6
6
8
12
18
3
13
2
16
9
4
1

$\mathrm{mod}\left[\left(x_i\right)^3 - x_i - 1, 23\right]$

-1
-1
5
0
13
4
2
13
20
6
0
8
13
21
15
1
8
19
17
8
21
16
22

$f23(x) := (x - 10)^2 \cdot (x - 3)$

$s231 := 3$

$s232 := 10$

$s233 := 10$

$f23(s231) = 0$

$f23(s232) = 0$

Type 3 primes factor in three linear equations

Based on the theorem from Lidl and Niederreiter above the order ord(f(x)) of the type 1,2, and 3 primes are respectively; p^2-1, $p^3-1 = (p^2+p+1)(p-1)$ and $p-1$.

The period length is related to the order of f(x), ord(f(x)), by the following theorem:

Let 3,0,2,3,2,5,5,... be the Perrin sequence in the field F_q with characteristic polynomial f(x) = x3 - x-1. Then the least period of the sequence divides ord(f(x)) based on the order of the type 1, 2 or 3 prime.

Corollary: The irreducible equation of f(x) divides $x^{ord(f(x)}-1$.

Example: Based on the above for p = 2 f(x) is irreducible so
ord(f(x) = $p^2+2+1 = 7$

$$\frac{x^7 - 1}{x^3 - x - 1} = x^4 + x^2 + x + 1 \mod 2$$

An observation of the number of solutions #E(q) and q

1. **For type 1 primes $(\#E(q)-q)^2 - 1 = 0 \mod 4$**
2. **For type 2 primes $(\#E(q)-q)^2 - 1 = 3 \mod 4$**

This observation extends to other elliptic curves for which the primes 2 and 23 are ramified.

Some Elliptic Curves with isomorphic modular form for type 1 and 2 primes mod 4

Weierstrass Form	Level or Conductor	Discriminant	Weierstrass Form	Level or Conductor	Discriminant
0,0,0,-1,-1	368	368	0,1,0,882,-4663	2116	$368*23^6$
0,1,0,-4,-5	368	368	0,1,1,-9698,446045	2116	$368*23^8$
0,1,0,0,-1	368	368	0,0,0 ,0,-220,-1256	1472	$23552= 23*2^{10}$
0,0,0,-55,157	368	368	0,1,0 ,0,7,-1	1472	23552
0,1,0,-18,-43	92	23^3*2^4	0,-1,0,0 -18,43	368	368*23^2
0,0,0,-1,1	92	368	0,0,0 ,0,-4,-8	1472	368
0,1,0,2,1	92	368	0,1,0 ,0-,73,271	1472	$(368)^2*4*23$

These concepts are applicable to communications, security, and encryption. Linear recurring sequences such as the Perrin and related sequences are important in security codes and random number generation.

RT