STATEMENTS OF CULMINATING SIGNIFICANCE FROM CLASS WORK ON THE PROJECTS

michael.fried@Colorado.edu michaeldavidfried@gmail.com

1. Solving Pell's Equation

Alex Oliver Alexander.Oliver@Colorado.edu
Erin Ruby Erin.Ruby@Colorado.edu
Logan Beck logan.beck@colorado.edu

I will show the historical progress on understanding solutions of

$$\{(x,y) \in R \mid P(x,y) = 0\} - P \text{ irreducible over } \mathbb{Q}.$$

Here R will have two cases $\mathbb{Z}$ and $\mathbb{Q}$. The distinction will be whether there are finitely or infinitely many solutions.

Further, I will first llustrate the major results with P running over just 3 cases:

$$P_{u,N} = x^u - Ny^u - 1, u = 2, 3, 4, \text{ with } N \text{ squarefree.}$$

1.1. $P_{2,N}$**: Pell's equation.** The group showed there were always infinitely many solutions. In my outline of the project, I showed the key idea in mathematics:

Break the goal into separate steps.

(1.1a) The box principle: Choose any large integer M. With each $b \leq M+1$, for some a, $|a - b\sqrt{N}| < 1$. So there two pairs (a,b) and (a',b') with $x = a - a'$, $y = b - b'$, $|x - y\sqrt{N}| < 1/M$.

(1.1b) For M in (1.1a), plug $\frac{x}{y}$ into Pell's equation and clear denominators for

$$|x^2 - Ny^2| \leq 3\sqrt{N} : \text{a finite number of } k \text{ values on the right side.}$$

(1.1c) From (1.1b), changing M, gives ∞-ly many solutions to the collection

$$\{x^2 - Ny^2 = k \mid k \leq 3\sqrt{N}\} : \text{For some } k = k', x^2 - Ny^2 = k' \text{ has } \infty\text{-ly many solutions.}$$

(1.1d) The Pell Equation project description noted that (1.1c) $\implies$ you have infinitely many pairs (x_i, y_i) of solutions of $x^2 - Ny^2 = k'$ with $x_i \mod k' \equiv a$ and $y_i \mod k' \equiv b$ constant (with i).

(1.1e) Take two of these, say (a_1, b_1) and (a_2, b_1) from (1.1d). Then

$$\Big(\frac{a_1 - \sqrt{N}b_1}{a_2 - \sqrt{N}b_2}\Big)\Big(\frac{a_1 + \sqrt{N}b_1}{a_2 + \sqrt{N}b_2}\Big) = \frac{k'}{k'} = 1.$$

Finally, just look separately at the left term $\frac{a_1 - \sqrt{N}b_1}{a_2 - \sqrt{N}b_2}$ multiplied by $\frac{a_2 + \sqrt{N}b_2}{a_2 + \sqrt{N}b_2}$. You get k' in the denominator, and $(a_1a_2 - b_1b_2N) + (a_1b_2 - a_2b_1)\sqrt{N}$ in the numerator.

The result, from (1.1d): Both coefficients are $\equiv 0 \mod k'$ and the result is $x' + y'\sqrt{N}$ with x' and y' are integers. Similarly with the left term, concluding finding integer solutions for Pell's equation.

The genus of $P(x,y)_{2,N}$ is 0. Diophantus' method showed it had infinitely many solutions in $\mathbb{Q}$. Now we know it has infinitely many solutions in $R = \mathbb{Z}$.

1.2. **Look at $P(x,y)_{3,N}$.** Its genus is 1. When you try (1.1a) on $N^{\frac{1}{3}}$ it won't work. Another diophantine result shows the truth goes in the other direction. This is the *Thue-Siegel-Roth Theorem*. The conclusion from this is that $P(x,y)_{3,N}$ has only *finitely* many solutions.

For $f(y)$ irreducible, $F(x,y)$ its homogenization, Thue-Siegel-Roth says [Mont91]:

$$|F(x,y)| > \max(|x|,|y|)^{d-2-\epsilon} \text{ for } \max(|x|,|y|) > C, C = C(f,\epsilon).$$

Immediately, if $g(x,y)$ has $\deg(g) < d-2$, then $F(x,y) = g(x,y)$ has $< \infty$-ly many integer solutions. Siegel (1938) eventually used this result to show that

$$\text{any } P(x,y) \text{ of genus} \geq 1 \text{ has only finitely many solutions in } \mathbb{Z}.$$

. This required immensely new ideas about how to treat algebraic equations based on Riemann's ideas.

1.3. **Look at $P(x,y)_{4,N}$.** It has genus > 1: its genus $\mathbf{g}$ is given by

$$2(4 + \mathbf{g} - 1) = 4 \cdot 3, \text{ or } \mathbf{g} = 3.$$

Faltings in the early 1980s showed what was then called Mordell's Conjecture.

$$\text{Any } P \text{ of genus} > 1 \text{ has only finitely many } \mathbb{Q} \text{ solutions.}$$

2. Projective Geometry

Sky Crastina Paul.Chrastina@Colorado.edu
Gouri Yerra goye8938@colorado.edu

2.1. **Context of so many perspectives.** Here is how I interpret the attempt of so many artists to show you the result of forcing different perspectives (from different points of view) into their works.

No one perspective works; but in some world you can see them all together.

The mathematical world is that of projective space, for which there is $\mathbb{CP}^1$, the projective line, $\mathbb{CP}^2$, the projective plane, and in general $\mathbb{CP}^n$, projective n-space.

2.2. **What remains when you change perspectives?** Alberti's view of points at ∞ represented a point of intersection of all lines parallel to a given one. The collection of points at ∞ from alberti's view becomes a line in the complex plane $\mathbb{CP}^2$, for which we can give coordinates by writing it as

$$L_z = \{(x,y,z) \neq \mathbf{0} \mid z = 0\}.$$

A curve, from a homogeneous equation $p(x,y,z) = 0$, in this plane will hit only finitely many of the points at ∞ unless when $z = 0$, $p(x,y,0)$ is always 0.

2.3. **Rational points.** On the points of $p(x, y, z) = 0$, there is no difference between talking about points over $\mathbb{Q}$ and points over $\mathbb{Z}$. Why? On, however,

$$C = \{(x, y)|p(x, y, 1) = P(x, y) = 0,$$

there is a big difference. If for example, the genus of C is 1 then there is never more than finitely many points in $\mathbb{Z}$ (Siegel's theorem, §1.2). Yet, there are many genus 1 such P for which there are ∞-ly many $\mathbb{Q}$ points.

The key is this. If we declare that $L_{a,b,c} = \{(x, y, z) \in \mathbb{CP}^2\}$ is the line at ∞, then the (projective) curve for $p(x, y, z) = 0$ restricted to $\mathbb{CP}^2 \setminus L_{a,b,c}$ – called the affine piece – can look very different than that for $P(x, y)$. Stillwell was talking about this when he said all the conic sections are really very similar, even though they don't look alike. Indeed, if $a, b, c \in \mathbb{Q}$, and if C has infinitely many $\mathbb{Q}$ points, then the affine piece on $\mathbb{CP}^2 \setminus L_{a,b,c}$ will also have ∞-ly many $\mathbb{Q}$ points.

3. Bezout's Theorem

Enrique Barraza enba2001@colorado.edu
Katrina Schwarzenberger Katrina.Schwarzenberger@Colorado.edu
Cullen Mchale David.Mchale@Colorado.edu

We never quite finished the connection between the resultant $r(x, z)$ and counting the number of points of intersection of two curves C_1 and C_2 given respectively by

$$C_i = \{(x, y, z) \in \mathbb{CP}^2 \mid p_i(x, y, z) = 0\}, i = 1, 2$$

with p_1 homogeneous of degree m and p_2 homogeneous of degree n.

Make this connection in the following case:

$$p_1 = y^m - u_1(x, z), p_2 = y^n - u_2(x, z),$$
$$u_1 \text{ homogenous of degree } m,\ u_2 \text{ homogenous of degree } n, \text{ in } x, z.$$

4. Group of an Equation

Yeshun Cheng Yechun.Cheng@Colorado.edu
Bernadette Montano Bernadette.Montano@Colorado.edu
Cortland Mchale Cortland.Mchale@Colorado.edu

4.1. **Groups and resulting mathematical directions.** I intended this presentation to lead into a discussion of the two roads on which mathematicians embarked in the years after Galois introduced his group G_P attached to an irreducible polynomial P over a field F.

- (4.1a) When $F = \mathbb{Q}$: The biggest immediate direction was toward investigating when G_P is abelian.
- (4.1b) When $F = \mathbb{C}(x)$: That direction was toward how to put together the equations P that give any group G as G_P.

Galois solved the famous problem: When can roots of P in case (4.1a) be written as functions from taking mth roots running over any possible m. His solution was that G_P is solvable. Solvable groups still have a mysterious place dividing abelian groups from simple groups; even which they are closer is not resolved, if you also exclude a special case of groups called *nilpotent* among the solvable groups.

Tieing the two topics of (4.1) together in the lectures was the idea that both benefited from using the appearance of the complex numbers $e^{\frac{2\pi i}{n}}$, solutions of

$y^n - 1$. The presentation on *Riemann and the Genus* took up (4.1b). The class lectures tried to use (4.1a) with the success of the Kronecker Weber theorem: all G_P abelian arose because the zeros of P where in the field $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ for some n.

4.2. **The project was intended to feature two parts.** Consider an irreducible polynomial P, of degree n, over $\mathbb{Q}$. Denote the complete collection of zeros of P by $y_1, \ldots, y_n$. Then, by substituting $y_{k'}$ for y_k in the vector space (over $\mathbb{Q}$)

$$L_{y_k} \stackrel{\text{def}}{=} \{\sum_{j=0}^{n-1} a_j y_k^j \mid a_j \in \mathbb{Q}\}$$

you get a vector space isomorphism $u_{k,k'} : L_{y_k} \to L_{y_{k'}}$ that sends the basis for L_{y_k} to the basis for $L_{y_{k'}}$. Every element in L_{y_k} is a polynomial $g(y)$ evaluated at y_k. [1] Then, these hold:

(4.2a) It is automatically a ring isomorphism – $g_1(y_k)g_2(y_k) \mapsto g_1(y'_k)g_2(y'_k)$.
(4.2b) From the Euclidean Algorithm, because P is irreducible, all elements (except 0) in the ring are invertible. So it is a field isomorphism.
(4.2c) It is easy to give examples, though, where Ly_k is different from $L_{y'_k}$.[2]

This idea of a vector space isomorphism is from your linear algebra course. All these vectors spaces, $k = 1, \ldots, n$, are in the complex numbers $\mathbb{C}$. Take all the sums and products of all the elements in the spaces $L_{y_1}, \ldots, L_{y_n}$. The result is still in $\mathbb{C}$, and it is called $\mathbb{Q}(y_1, \ldots, y_n)$. It is a vector space, too, containing all the vector spaces L_k. The project described finding a linear combination $\alpha = sum_1^n a_k y_k$ (a_k s in $\mathbb{Q}$) of $y_1, \ldots, y_n$ for which:

$$\text{with } y_1 \text{ replaced by } \alpha \; L_\alpha = \mathbb{Q}(y_1, \ldots, y_n).$$

The primitivity condition:: Such an α_1 is called a primitive element. Then, $\alpha = \alpha_1$ satisfies an irreducible polynomial, P_α. Elements of Galois' group, G_P, correspond to the roots $\alpha_1, \ldots, \alpha_N$ of P_α with $\deg(P_\alpha \stackrel{\text{def}}{=} N)$ by mapping $\alpha_1 \to \alpha_k$ because this maps $\mathbb{Q}(y_1, \ldots, y_n)$ onto itself, permuting the zeros, $y_1, \ldots, y_n$, of P.

That is, any element $\tau \in G_P$ is a permutation of $y_1, \ldots, y_n$, and so an element of S_n. Importantly, for some P not all permutations of S_n are in G_P. That happens exactly when $N < n!$.

(4.3a) Use $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ as an example of when the primitivity condition holds.
(4.3b) Actually consider – in special cases – what is the group G_{P_n} if P_n is the irreducible factor of $y^n - 1$ having $\alpha_n \stackrel{\text{def}}{=} e^{\frac{2\pi i}{n}}$ as a zero.

Yechun considered, in particular ways, both topics. My comments enhance his two topics. In class we learned that in case (4.3) G_P is a subgroup of the integers prime to n, $G \stackrel{\text{def}}{=} (\mathbb{Z}/n)^*$, an abelian group under multiplication. For $n = p^2$ with p an odd prime, the order of this group – number of elements – is $p^2 - p = (p-1)p$. In class we discussed – using very simple algebra – the following topics.

(4.4a) If there is $\tau_1, \tau_2 \in G$ with the order of τ_1 ($\text{ord}(\tau_1)$) equal $p - 1$ and $\text{ord}(\tau_2) = p$, then $\tau = \tau_1\tau_2$ has order $p^2 - p$.

[1] This is the analog of how we substituted $-\sqrt{N}$ for $\sqrt{N}$ when we discussed Pell's equation.

[2] Hint: This is the case for $y^3 - N$, with N any cube-free integer where y_1 is the real root. Why?

(4.4b) From (4.4a) G is generated by τ and so it is a cyclic group.
(4.4c) Further, if another group G^* is cyclic of order $p^2 - p$, then it contains elements of τ_1 and τ_2 with their orders given in (4.4a). Why?
(4.4d) Finally, all of the groups $\mathbb{Z}/p^u$, $u \geq 2$ have an element of order p^{u-1}.[3]

5. Riemann and the Genus

Haotian Peng Haotian.Peng@Colorado.edu
Yuehua Yang Yuehua.Yang@Colorado.edu
Zihan Zhou Zihan.Zhou@Colorado.edu

This starts by saying that given any equation $p(x, y, z)$ – homogeneous – defining an irreducible curve in $\mathbb{CP}^2$, there is a map of that curve to $\mathbb{CP}^1$ defining its genus using fractional power series for the finite number of values that arise from a resultant as in Bezout's Theorem.

Further, this also gives Galois's group of the equation, and elements in the group – arising from those fractional power series – that generate it, and have product one. What I will do here is use the definitions and see what the inverse theorem of Riemann says that answers the question given to this project.

5.1. **Applying Riemann's Theorem.** We apply it to the case $G = A_5$ to product an irreducible polynomial $P(x, y)$ that defines a curve of genus 0, for which G_P – Galois' group – is A_5 when you regard P as a polynomial with coefficients in $\mathbb{C}(x)$.

Riemann says that given any group G and some elements $\tau_1, \ldots, \tau_r$ in the group that *generate it* and have *product one*, you get a curve in $\mathbb{CP}^2$ from which all this comes by using fractional power series. I suggested trying $r = 4$ and using all of $\tau_1, \ldots, \tau_r$ to be 3-cycles. We aren't proving Riemann's Theorem. We are just trying to find these τ s so that Riemann's Theorem applies.

What we have to find is four τ s of the form $(i\, j\, k)$ with these properties:

(5.1a) Product-one: $\tau_1\tau_2\tau_3\tau_4 = 1$, and;
(5.1b) Generation: Every element in A_5 is a product of these τ s.

Once we have found those, Riemann's Theorem does the rest.

5.2. **Finding those τ s.** Try these elements for the τ s:

$$\boldsymbol{\tau} = (\tau_1 = (1\,2\,3), \tau_2 = (1\,3\,2) = \tau_1^{-1}, \tau_3 = (3\,4\,5), \tau_4 = \tau_3^{-1}).$$

Notice their product is already 1, so you have only to show the group they generate is A_5. There are only three kinds of elements in A_5, besides the identity; Elements of order 5 – 5-cycles; of order 3 –3-cycles; and of form $(i\, j)(k\, l)$–product of 2 disjoint 2-cycles. Denote the group generated by τ_1, τ_2 by G.

By conjugating τ_1 by powers of τ_2 and get $(1\,2\,k)$ with $k = 3, 4, 5$. By conjugating the last by τ_1 we get $(2\,3\,k)$ with $k = 4$ or 5. By taking inverses of these elements, we get all possible 3-cycles in G.

Now that you have all 3-cycles, just check that $\tau_1\tau_2 = (1\,2\,3\,4\,5)$. From this by changing the 3-cycles, you can write any 5-cycle as a product of 3-cycles. Similarly, write $(2\,3)(1\,4)$ as $\tau_1(1\,2\,4)$.

[3]Hint: Use the binomial theorem on $1 + p$ to check that p^{u-1} is the smallest power of it congruent to 1 mod p^u.

5.3. **Now consider using the genus formula.** This is a separate problem from the above. Take $P^* = P(y) - x$ and $p(x, y, z) = z^{\deg(P)}(P(y/z) - (x/z))$, with P a degree 5 polynomial.

(5.2a) What are the elements in S_5 that commute with $\tau = (1\,2\,3\,4\,5)$, a 5-cycle?

(5.2b) In class we learned the branch cycle at ∞ for polynomial is a 5-cycle. That means G_{P^*} contains a 5-cycle.

(5.2c) We learned in another exercise that the genus of the curve defined by $p(x, y, z)$ is 0.

(5.2d) Assume G_{P^*} is abelian. Conclude from the genus formula that

$$\{(x, y, z) \in \mathbb{CP}^2 \mid p(x, y, z) = 0\} \to \mathbb{CP}^1, \text{ by } (x, y, z) \mapsto (x, z).$$

has only 1 branch point other than ∞.

(5.2e) Conclude further: therefore G_{P^*} is cyclic of order 5.[4]

6. Diophantine Undecidability

Matthew LeMay Matthew.Lemay@Colorado.edu
Kristopher Holmquist Kristofer.Holmquist@Colorado.edu
Logan Tromly lotr4143@Colorado.edu

References

[Mont91] I. Niven, H. Zukerman, H. Montgomery, *An introduction to the Theory of Numbers*, 5th Edition, J. Wiley and Sons, 1991.

[4]Hint: Use the product-one condition.