The rationality of conics over finite fields
(And an introduction to rational normal curves and classical Goppa codes)

Hypersurfaces in projective space. Fix a ground field F. Projective space $\mathbf{P}^{k-1}(F)$ of dimension $k-1$ has coordinates $(x_1 : x_2 : \ldots : x_k)$ that are defined only up to scaling: we have $(x_1 : x_2 : \ldots : x_k) = (cx_1 : cx_2 : \ldots : cx_k)$ for all $c \in F^*$. Thus in general it does not make sense to evaluate a rational function of the x_i at $(x_1 : x_2 : \ldots : x_k)$. Functions invariant under scaling are "homogeneous of degree zero", but a nonconstant homogeneous rational function must have denominators (and worse, how to evaluate x_1/x_2 when $x_1 = x_2 = 0$?). If we limit ourselves to polynomials $P(x_1, x_2, \ldots, x_k)$ then the best we can do is to make P homogeneous of some degree d. Then (unless $d = 0$) it still doesn't make sense to evaluate P at $(x_1 : x_2 : \ldots : x_k)$,[1] but *zeros* of P are well-defined: if $P(x_1, \ldots, x_k) = 0$ then also $P(cx_1, \ldots, cx_k) = 0$ for all c. The set of $(x_1 : x_2 : \ldots : x_k) \in \mathbf{P}^{k-1}$ at which a given nonzero polynomial of degree $d > 0$ vanishes is called a "hypersurface of degree d". For $k = 2, 3, 4$ we don't usually call it a hypersurface because it's just a finite set of points, a curve, or a surface in the projective line, plane, or space respectively. For $d = 1$ this is a hyperplane (or point, line, plane for $k = 2, 3, 4$); for $d = 2$ it is called a quadric, and for $d = 3, 4, 5$, etc., we indicate the degree of the hypersurface by the same word that applies to the polynomial: cubic, quartic, quintic, etc. (A homogeneous polynomial is often called a "form", as in linear form [= linear functional], quadratic form, cubic form, etc.; the number of variables is indicated by the adjective binary, ternary, quaternary, "etc.", so for example a conic is the zero-locus of a "ternary quadratic form", a.k.a. "ternary quadric".)

Conics. A quadric (degree-2 curve) $P(x_1, x_2, x_3) = 0$ in $\mathbf{P}^2$ is called a "conic", because the conic sections of classical Greek geometry are all quadric curves in $\mathbf{P}^2(\mathbf{R})$ (excluding their points at infinity if any, because the Greeks worked only in $\mathbf{R}^2$; and conversely any quadric curve with $F = \mathbf{R}$ is a conic section as long as its set of real points is nonempty). In this degree and dimension, the locus of $P = 0$ is smooth *iff* P is irreducible over $\overline{F}$. Recall that a solution $\vec{x} = (x_1 : x_2 : \ldots : x_k)$ is "smooth" if P vanishes only to order 1 at $\vec{x}$, or equivalently, if at least one of the partial derivatives of P is nonzero at $\vec{x}$. (Yes, this criterion is well-defined: for $c \in F^*$ it holds at $c\vec{x}$ *iff* it holds at $\vec{x}$.) Now if P factors then $P = L_1 L_2$ for some linear forms L_1, L_2; but then $L_1 = 0$ and $L_2 = 0$ are lines in $\mathbf{P}^2$, which meet at a point (or worse, are the same), and P vanishes to order 2 at a point p such that $L_1(p) = L_2(p) = 0$. [Note that L_1 and L_2 may be quadratic conjugates, but their intersection still has a representative with rational coordinates. Think of the example $F = \mathbf{R}$, $P(x_1, x_2, x_3) = x_1^2 + x_2^2$, when L_1, L_2 are $x_1 \pm ix_2$ and both vanish at $(0 : 0 : 1)$.] Conversely, suppose $\vec{x}$ is a singular point of $P = 0$, and choose coordinates so $\vec{x} = (0 : 0 : 1)$. Then $P = a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2$, which factors as a product of two linear forms.

Now suppose C is a smooth conic $P(x_1, x_2, x_3) = 0$, and l is any line $L(x_1, x_2, x_3) = 0$. Then $C \cap l$ contains at most two points, even over $\overline{F}$. Indeed the restriction of P to l is a *nonzero* quadratic form in two variables (it cannot be identically zero because P is irreducible). Thus $C(F)$ (the set of points of C in $\mathbf{P}^2(F)$) is an "arc": a subset of $\mathbf{P}^2(F)$ containing no three collinear points. We shall show that if F is finite then $C(F)$ consists of exactly $q + 1$ points, and is thus an oval. For now we shall show that given C and a point $p_0 \in C(F)$ there is a natural bijection between $C(F)$ and the lines through p_0; this will prove the $q + 1$ formula once we've shown that $C(F)$ contains at least one point.

Warning: for general F the existence of p_0 is not at all guaranteed! Already in the familiar case $F = \mathbf{R}$ there are counterexamples, such as $P(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$, which is irreducible but yields a "pointless" conic C. When $F = \mathbf{R}$ this pointless conic is unique up to $\mathrm{PGL}_3(F)$ isomorphism; but when $F = \mathbf{Q}$, or more generally

[1] Though it *does* make sense to ask what $P(x_1, \ldots, x_k)$ is modulo d-th powers, and even $P(x_1, \ldots, x_k)$ makes sense if we're in a finite field of q elements with $q - 1 \mid d$. We shall use the case $d = q - 1$ in the final paragraph.

a "number field" (a field containing $\mathbf{Q}$ that is finite-dimensional as a $\mathbf{Q}$-vector space, such as $\mathbf{Q}[i]$ or $\mathbf{Q}[\sqrt{2}]$ or even $\mathbf{Q}[\sqrt[5]{2}]$), there are various ways that C can fail to have rational points (try $x_1^2 + 2x_2^2 - 5x_3^2$ with $F = \mathbf{Q}$), which give rise to quite a rich picture which encompasses Quadratic Reciprocity and more; but none of these complications will arise for F finite.

The bijection π between points on C and lines through $p_0 \in C$ generalizes the classical parametrization of Pythagorean triples, i.e. of rational points on the conic $x_1^2 + x_2^2 - x_3^2 = 0$, starting from a known point such as $(-1 : 0 : 1)$. Geometrically, π is projection from p_0. That is, if $p \neq p_0$ then $\pi(p)$ is just the line joining p to p_0. (We've seen already that this line determines p uniquely.) This leaves only one point and one line unaccouneted for: p_0 itself, and the one line through p_0 that has no other intersection with C, namely the *tangent line* t_{p_0} at p_0. So we declare that π takes p_0 to t_{p_0}. That makes sense algebraically too: restricting P to t_{p_0} yields a quadratic polynomial that vanishes to order 2 at p_0 (geometrically, t_{p_0} intersects C with multiplicity 2 at p_0); so we can define π^{-1} in general by saying that for an line $l \ni p_0$ the conic intersects l at p_0 and $\pi^{-1}(l)$, and that's true even for $l = t_{p_0}$ when we interpret "at p_0 and p_0" as "at p_0 with multiplicity 2".

To do this explicitly, we can choose coordinates so $p_0 = (1 : 0 : 0)$, so $P(x_1, x_2, x_3)$ has the form $a_{12}x_1x_2 + a_{13}x_1x_3 + P_0(x_2, x_3)$ for some binary quadratic form P_0, with a_{12} and a_{13} not both zero (lest p_0 be a singular point). By linear change of coordinates on x_2 and x_3 we may assume $a_{12} = 0$, and then scale to $a_{13} = -1$; geometrically this makes t_{p_0} the "line at infinity" $x_3 = 0$. Now

$$P(x_1, x_2, x_3) = P_0(x_2, x_3) - x_1x_3 = a_{22}x_2^2 + a_{23}x_2x_3 + a_{33}x_3^2 - x_1x_3,$$

with $a_{22} \neq 0$ because P is not a multiple of x_3. We may now write an arbitrary line l through p_0 other than t_{p_0} as $x_2 = rx_3$, getting $P = x_3(a_{22}r^2 + a_{23}r \ + a_{33} - x_1)$ on l, and thus

$$(x_1 : x_2 : x_3) = (a_{22}r^2 + a_{23}r \ + a_{33} : r : 1).$$

The point p_0 is then obtained from this by setting "$r = \infty$"; that is, we can think of the set of lines through p_0 as a projective line $\mathbf{P}^1$ with coordinate $(r : 1)$, and then π is a bijection from $\mathbf{P}^1$ to C that takes $(r_1 : r_0)$ to

$$(x_1 : x_2 : x_3) = (a_{22}r_1^2 + a_{23}r_0r_1 + a_{33}r_0 : r_0r_1 : r_0^2),$$

which agrees with the previous formula when $(r_1, r_0) = (r, 1)$, and becomes $(1 : 0 : 0)$ when we take $(r_1, r_0) = (1, 0)$ (recall that $a_{22} \neq 0$).

[*Remark*: Note that the formula for $(x_1 : x_2 : x_3)$ is well-defined, even though (r_1, r_0) are defined only up to scaling, because multiplying each of r_1, r_0 by the same scalar λ multiplies each x_i by the same factor λ^2 and thus yields the same point $(x_1 : x_2 : x_3)$ in projective space. We must also check that x_1, x_2, x_3 cannot all vanish at the same $(r_1 : r_0)$, but that's guaranteed by $a_{22} \neq 0$. This illustrates a key technique for mapping algebraic varieties to projective space via "sections of line bundles"; but in Math 256 we shall say no more about this technique in anything like full generality.]

By a final linear change of variable on $\mathbf{P}^2$ we identify C with the conic $x_2^2 - x_1x_3 = 0$, parametrized by $(r_1^2 : r_0r_1 : r_0^2)$. This means that *all conics with a rational point are equivalent* under the group $\mathrm{PGL}_3(F)$ of projective linear transformations of $\mathbf{P}^2$. Since our choice of p_0 was arbitrary, we've even shown that all points on C are equivalent under the stabilizer of the conic in $\mathrm{PGL}_3(F)$. We shall see that in fact the stabilizer is just the group $\mathrm{PGL}_2(F)$ of projective linear transformations of the projective line with coordinates $(r_1 : r_0)$, and thus acts simply 3-transitively on the points of C. But first we shall count the smooth conics in $\mathbf{P}^2(F)$ when F is finite.

Exercise: Suppose $F = \mathbf{Q}$ and let C be the circle $x_1^2 + x_2^2 = x_3^2$. Carry out this procedure for $p_0 = (-1 : 0 : 1)$. You should obtain a formula that's plainly equivalent with the well-known parametrization $(x_1 : x_2 : x_3) = (m^2 - n^2 : 2mn : m^2 + n^2)$ of Pythagorean triples.

Enumeration of smooth conics. Now that we know that a conic over a finite field of q elements has either 0 or $q+1$ points, one strategy for showing that the former never occurs is to count the conics with rational points and compare our answer with the overall count of conics. We obtain the overall count as follows.

Proposition. *Let F be a finite field of q elements. Then there are $q^5 - q^2$ smooth conics in $\mathbf{P}^2(F)$.*

Proof: We enumerate all the conics and then subtract the degenerate ones. A conic is the zero-locus of a quadratic form $P(x_1, x_2, x_3)$ in 3 variables; the vector space of such forms has dimension 6, so the conics constitute a projective space $\mathbf{P}^5(F)$, with $q^5 + q^4 + q^3 + q^2 + q + 1$ points. Of these, $q^2 + q + 1$ are double lines, $P = cL^2$ for some nonzero linear form L and field element c. The remaining singular conics are $P = L_1 L_2$ for some non-proportional linear forms L_1, L_2, either both defined over F or quadratic conjugates over $\overline{F}$, and in either case meeting at a point $p \in \mathbf{P}^2$ rational over F. There are $q^2 + q + 1$ choices for p_0, all equivalent under $\mathrm{Aut}(\mathbf{P}^2(F))$, so each contributes the same number of singular conics. For $p_0 = (0:0:1)$, the space of P vanishing to order (at least) 2 at p_0 is $\{a_{11}x_1^2 + a_{12}x_1x_2 + a_{22}x_2^2 : a_{11}, a_{12}, a_{22} \in F\}$. Excluding zero and identifying proportional polynomials yields a 2-dimensional projective plane of P's, so there are $q^2 + q + 1$ such conics. But again these include some "double lines" cL^2, this time with $q+1$ choices of L vanishing at p_0 up to scaling. This leaves q^2 conics singular only at p_0, and thus $q^4 + q^3 + q^2$ singular conics with a unique singular point. Subtracting this from our count of $q^5 + q^4 + q^3$ conics that are not double lines yields $q^5 - q^2$ as claimed. $\diamondsuit$

There are several ways to proceed now. The most natural for us may be to count ordered quadruples (C, p_1, p_2, p_3) where C is a smooth conic and p_1, p_2, p_3 are pairwise distinct points on C, because we've already used triply-marked conics in the proof of Segre's theorem. Let N be that count. If C is a conic with rational points then there are $(q+1)q(q-1) = q^3 - q$ choices for (p_1, p_2, p_3). Thus the number of conics with points is $N/(q^3 - q)$. On the other hand, N is the sum over p_1, p_2, p_3 of conics passing through each p_i. Necessarily the p_i are not collinear, and we already know that $\mathrm{PGL}_3(F)$ acts transitively on ordered 3-arcs, so we need only enumerate the conics for one choice of p_1, p_2, p_3 and then multiply by the number $(q^2 + q + 1)(q^2 + q)q^2$ of ordered 3-arcs. As before we place p_i at the unit vectors $(1:0:0)$, $(0:1:0)$, $(0:0:1)$. Then a quadric $P(x_1, x_2, x_3)$ vanishes on all three p_i *iff* it is of the form $a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3$, and then P is irreudcible *iff* none of the a_{ij} vanishes. Since proportional P yield the same conic, the desired count is $(q-1)^2$, and we find that

$$\frac{N}{q^3 - q} = \frac{(q^2 + q + 1)(q^2 + q)q^2(q-1)^2}{q^3 - q} = \frac{(q^3 - 1)(q^3 - q)q^2}{q^3 - q} = q^5 - q^2.$$

Since that agrees with our previous count, we conclude that every smooth conic over F has at least one rational point, and thus exactly $q+1$ rational points.

Remark: For the non-smooth conics, the double lines also have $q+1$ points, but the line-pairs have $2q+1$ or 1 according as the component lines are individual rational or Galois-conjugate. For that matter the zero quadric has q^2+q+1 points. Still, it is true that for *every* quadric $P(x_1, x_2, x_3)$ the number of points in $\mathbf{P}^2(F)$ satisfying $F = 0$ is $\equiv 1 \bmod q$; equivalently, the number of solutions of $P(x_1, x_2, x_3) = 0$ in F^3 (without scaling or even excluding the trivial solution $(0,0,0)$) is a multiple of q. If we could show this directly then we would have an alternative proof that there are no pointless conics over a finite field. There is in fact a general result on the number of points in hypersurfaces, which includes the $1 \bmod q$ congruence as a special case; but we won't be able to prove it this term except for the case $q = 2$. But there is a weaker result that's good enough: Chevalley's theorem that over a finite field of characteristic p the number of zeros of a degree-d form in more than d variables is a multiple of p. This proof we can give without too much difficulty, and will do so later this term.

Since we have also seen that all smooth conics with a rational point are equivalent under $\mathrm{PGL}_3(F)$,

we can now also compute the size of the stabilizer when F is finite: it is

$$\frac{\#\,\mathrm{PGL}_3(F)}{q^5-q^2} = \frac{(q^3-1)(q^3-q)(q^3-q^2)/(q-1)}{q^5-q^2} = q^3-q.$$

This is the same as $\#\,\mathrm{PGL}_2(F)$ for good reason: over any field, the stabilizer in $\mathrm{PGL}_3(F)$ of a smooth conic with a rational point is *isomorphic* with the group $\mathrm{PGL}_2(F)$ of projective linear transformations of the $(r_1 : r_0)$ line. We have seen that the conic is parametrized by $(r_1^2 : r_0 r_1 : r_0^2)$, where the coordinates form a basis for the space of *all* homogeneous binary quadrics; any linear change of variables $(r_1 : r_0) \mapsto (ar_1 + br_0, cr_1 + br_0)$ simply yields a different basis for that space, and is thus realized by a projective linear transformation of $\mathbf{P}^2$ that fixes the locus of $x_1x_3 = x_2^2$. Explicitly, this linear tranformation has matrix

$$\begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}.$$

Can you explain why the determinant of this matrix is just the cube $(ad-bc)^3$ of $\det(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})$? [Hint: it's a *homomorphism* from $\mathrm{PGL}_2(F)$ to $\mathrm{PGL}_3(F)$.]

Rational normal curves. More generally, if instead of all degree-2 monomials in r_1, r_0 we use all monomials of degree d, we get the map

$$(r_1 : r_0) \mapsto (r_1^d : r_0 r_1^{d-1} : r_0^2 r_1^{d-2} : \cdots : r_0^d)$$

from $\mathbf{P}^1$ to $\mathbf{P}^d$, whose image is called the *rational normal curve of degree* d in $\mathbf{P}^d$. (It has "degree d" because it meets any hyperplane in d points over $\overline{F}$, counted with multiplicity.) Thus $\mathbf{P}^1$ itself is the rational normal curve of degree 1, and a conic with a rational point is a rational normal curve of degree 2. The $d = 3$ case is usually known as the "twisted cubic curve" in $\mathbf{P}^3$, and can be defined by the equations $x_1x_3 - x_2^2 = x_1x_4 - x_2x_3 = x_2x_4 - x_3^2 = 0$.

Classical Goppa codes. Over a finite field F of q elements, the points of a rational normal curve of degree d are $q+1$ points in general linear position in $\mathbf{P}^d$, and thus yield a $[q+1, d+1, q-d+1]$ MDS code. Such an MDS code is called a "classical Goppa code" ("classical" to distinguish it from a generalization where $\mathbf{P}^1$ is replaced by a more complicated algebraic curve; the non-classical codes are no longer MDS, but can have arbitrarily large length n). Unwinding the construction, we see that the codewords are homogeneous polynomials of degree d "evaluated" at each of the $q+1$ points of $\mathbf{P}^1$ — there is no canonical way of doing this, but all choices are isomorphic as code. One standard choice is to use $r = r_1/r_0$ as before and identify homogeneous degree-d polynomials with ordinary polynomials $P(r)$ of degree at most d; then q of the coordinates are the values of P at the q field elements, and the $(q+1)$st coordinate is the r^d coefficient of P, which plays the role of $P(\infty)$.

The dual of a classical Goppa code is again a classical Goppa code of complementary parameters $[q+1, q-d, d+1]$ coming from polynomials of degree $q-d-1$. Because the dimensions match, we can prove this duality by checking that $\sum_{(r_1:r_0)\in\mathbf{P}^1(F)} P(r_1,r_0)Q(r_1,r_0) = 0$ for all homogeneous binary forms P, Q of degrees $d, q-d$ respectively. The summand is well-defined because $\deg(PQ) = q-1$ and every $\lambda \in F^*$ satisfies $\lambda^{q-1} = 1$. So an equivalent claim is $\sum_{(r_1,r_0)\in F^2-\{(0,0)\}} P(r_1,r_0)Q(r_1,r_0) = 0$, and we may as well include the $(r_1, r_0) = (0,0)$ term. The result is then proved termwise from the expansion of PQ in monomials. This technique will recur in the proof of Chevalley's theorem.