The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point

Manjul Bhargava, John Cremona, and Tom Fisher

16th July 2015

Abstract

We show that the proportion of plane cubic curves over $\mathbb{Q}_p$ that have a $\mathbb{Q}_p$-rational point is a rational function in p, where the rational function is independent of p, and we determine this rational function explicitly. As a consequence, we obtain the density of plane cubic curves over $\mathbb{Q}$ that have points everywhere locally; numerically, this density is shown to be $\approx 97.3\%$.

1 Introduction

Any plane cubic curve over $\mathbb{Q}$ may be defined by the vanishing of a ternary cubic form

$$C(X,Y,Z) = aX^3 + bX^2Y + cX^2Z + dXY^2 + eXYZ + fXZ^2 + gY^3 + hY^2Z + iYZ^2 + jZ^3 \quad (1)$$

where all coefficients $a, \ldots, j$ lie in $\mathbb{Z}$. We say that a ternary cubic form C is *everywhere locally soluble* if it has a nontrivial zero over every completion of $\mathbb{Q}$, i.e., if the corresponding plane cubic curve has a point everywhere locally. In this paper, we wish to determine the probability that a random such integral ternary cubic form is everywhere locally soluble.

More precisely, define the height $h(C)$ of the cubic form C in (1) by $h(C) := \max\{|a|, \ldots, |j|\}$. Then, as in the work of Poonen and Voloch [11], we define the probability that a random plane cubic curve over $\mathbb{Q}$ has a point everywhere locally (equivalently, the probability that a random integral ternary cubic form is everywhere locally soluble) by

$$\rho = \lim_{B\to\infty} \frac{\#\{C(X,Y,Z) : C \text{ is everywhere locally soluble and } h(C) < B\}}{\#\{C(X,Y,Z) : h(C) < B\}}.$$

It is proven in [11, Thm. 3.6], using the sieve of Ekedahl [7], that this limit exists and is given by

$$\rho = \prod_p \rho(p), \quad (2)$$

where the product is over all primes p; here $\rho(p)$ denotes the probability (with respect to the usual additive $\mathbb{Z}_p$-measure) that a random ternary cubic form over $\mathbb{Z}_p$ is *soluble* over $\mathbb{Q}_p$, i.e., has a nontrivial zero over $\mathbb{Q}_p$. There is no contribution from the infinite place because a plane cubic curve over $\mathbb{R}$ always has real points.

While the methods of [11] prove the existence of ρ, the equality (2), and the inequality $0 < \rho < 1$, they do not indicate how to *compute* the values $\rho(p)$ or what form these values might take. The purpose of this article is to develop a method to determine the probabilities $\rho(p)$ for all primes p, and thus ρ, explicitly. Specifically, we will prove that $\rho(p)$ is a rational function in p, where the rational function is independent of p:

Theorem 1 *The probability that a random plane cubic curve over $\mathbb{Q}_p$ has a $\mathbb{Q}_p$-rational point is given by*

$$\rho(p) = 1 - \frac{f(p)}{g(p)}$$

where f and g are the following integer coefficient polynomials of degrees 9 and 12:

$$f(p) = p^9 - p^8 + p^6 - p^4 + p^3 + p^2 - 2p + 1,$$
$$g(p) = 3(p^2+1)(p^4+1)(p^6+p^3+1).$$

Note that $1 - \rho(p) = f(p)/g(p) \sim 1/(3p^3)$, so $\rho(p) \to 1$ rapidly as $p \to \infty$; for small p, we have $\rho(2) \approx 0.98319$, $\rho(3) \approx 0.99259$, $\rho(5) \approx 0.99795$, and $\rho(7) \approx 0.99918$.

From Theorem 1, we conclude:

Theorem 2 *The probability that a random plane cubic curve over $\mathbb{Q}$ has a point locally everywhere is given by*

$$\rho = \prod_p \rho(p) = \prod_p \left(1 - \frac{f(p)}{g(p)}\right).$$

Numerically, we have $\rho \approx 97.256\%$. Thus the probability that a random plane cubic curve over $\mathbb{Z}$ has a point everywhere locally is very high.

Although we have stated Theorem 2 for plane cubic curves ordered by their height, we note that the same result also holds for more general orderings, as we now explain. Let D be a piecewise smooth rapidly decaying function on the vector space $\mathbb{R}^{10}$ of real ternary cubic forms (i.e. $D(x)$ and all its partial derivative are $o(|x|^{-N})$ for all $N > 0$), and assume that $\int D(C)dC = 1$; we call such a function D a *nice distribution* on the space of real ternary cubic forms. Then we define the probability, with respect to the distribution D, that a random ternary cubic form C is everywhere locally soluble (ELS) to be

$$\rho^D = \lim_{X\to\infty} \frac{\sum_{C \text{ integral, ELS}} D(C/X)}{\sum_{C \text{ integral}} D(C/X)}.$$

In the case D is the indicator function for the box $[-1/2, 1/2]^{10}$, this is the same as the probability ρ defined above. The arguments in [3, Section 2], stated there for quadratic forms, carry over immediately to cubic forms. Since for cubic forms the probability of solubility over the reals is always 1, it follows that $\rho^D = \prod_p \rho(p)$ for all nice distributions D. In particular ρ^D is independent of D.

Our result that $\rho(p)$ is a rational function of p independent of p is special to plane cubic curves, as it does not always occur in other contexts. For example, for the genus one models $y^2 = f(x, z)$, where f is a binary quartic form over $\mathbb{Z}$ (or more generally, a binary form of degree $2g + 2$ yielding a hyperelliptic curve of genus g), we show in [4] that the analogue of $\rho(p)$ is not any fixed rational function of p. Nonetheless our approach in [4] to computing the probabilities $\rho(p)$ for the genus one

models $y^2 = f(x, z)$ follows that of this paper, and it is an interesting question to determine in what generality our methods apply.

Our strategy for proving Theorem 1 is based on that for testing solubility of a smooth plane cubic over $\mathbb{Z}_p$ (equivalently, $\mathbb{Q}_p$) as described, for example, in [8, Section 2]; the arguments are also related to those used for minimising ternary cubics, as in [5], and of those used to determine the density of isotropic integral quadratic forms, as in [3]. Namely, we consider the reductions modulo p of these ternary cubic forms; cubics whose reductions have smooth $\mathbb{F}_p$-points are soluble by Hensel's Lemma, while those that have no $\mathbb{F}_p$-points are insoluble. In order to determine the probabilities of solubility in the more difficult remaining cases, we develop certain recursive formulae, involving these and other suitable related quantities, that allow us to solve and obtain exact algebraic expressions for the desired probabilities.

The result of Theorem 2 also plays an important role in [1], where it is shown that a positive proportion of locally soluble plane cubic curves over $\mathbb{Q}$ do not possess a rational point (i.e., fail the Hasse principle), while a positive proportion do possess a rational point. It is also conjectured there (using Theorem 2, along with other considerations from the geometry of numbers) that the probabililty that a random plane cubic has a rational point is $(1/3)\prod_p \rho(p) \approx 32.419\%$.

We remark that the analogue of Theorem 1 holds (with the same proof) over any finite extension of $\mathbb{Q}_p$; we simply replace p by a uniformiser when making substitutions in the proofs, and replace p by the order of the residue field when computing probabilities. The analogue of Theorem 2 then also holds with any number field in place of $\mathbb{Q}$ (where we define the relevant probability following [11, §4]).

This paper is organized as follows. In Section 2, we provide basic counts of some polynomials and forms over finite fields that are required in the proof of Theorem 1. In Section 3, we then develop the recursive formulae described above, and use these formulae to prove Theorem 1. In Section 4, we give an extension of Theorem 1 where we determine the probability that a random plane cubic curve over $\mathbb{Q}_p$ has a point over some unramified extension of $\mathbb{Q}_p$. We find that the answer takes a particularly simple form in this case, and we outline the necessary changes required for the proof. Finally, in Section 5, we give some concluding remarks and describe some related problems of interest.

2 Some counting over finite fields

We work over the finite field $\mathbb{F}_q$ with q elements, where q is a prime power.

2.1 Cubic polynomials and binary cubic forms over $\mathbb{F}_q$.

Lemma 3 *Of the q^3 monic cubics $g \in \mathbb{F}_q[X]$,*

- *$q^2(q-1)$ have distinct roots, of which*
  - *$\frac{1}{6}q(q-1)(q-2)$ have distinct roots in $\mathbb{F}_q$;*
  - *$\frac{1}{2}q^2(q-1)$ have one root in $\mathbb{F}_q$ and two conjugate roots in $\mathbb{F}_{q^2}$;*
  - *$\frac{1}{3}q(q^2-1)$ have three conjugate roots in $\mathbb{F}_{q^3}$;*
- *$q(q-1)$ have a simple root and a double root (both in $\mathbb{F}_q$);*
- *q have a triple root (in $\mathbb{F}_q$).*

Corollary 4 *The probability that a random monic cubic over $\mathbb{F}_q$ has a simple root in $\mathbb{F}_q$ is $\sigma_1 = \frac{2}{3}(q^2-1)/q^2$, and the probability that it has a triple root is $\tau_1 = 1/q^2$.*

Lemma 5 *Of the q^4 binary cubic forms $g \in \mathbb{F}_q[X,Y]$,*

- $q(q^2-1)(q-1)$ *have distinct roots, of which*
  - $\frac{1}{6}q(q^2-1)(q-1)$ *have all three roots in $\mathbb{F}_q$;*
  - $\frac{1}{2}q(q^2-1)(q-1)$ *have one root in $\mathbb{F}_q$ and two conjugate roots in $\mathbb{F}_{q^2}$;*
  - $\frac{1}{3}q(q^2-1)(q-1)$ *have three conjugate roots in $\mathbb{F}_{q^3}$;*
- $q(q^2-1)$ *have a simple and a double root (both in $\mathbb{F}_q$);*
- q^2-1 *have a triple root (in $\mathbb{F}_q$);*
- 1 *is the zero form.*

Corollary 6 *The probability that a random binary cubic form over $\mathbb{F}_q$ has a simple root in $\mathbb{P}^1(\mathbb{F}_q)$ is $\sigma = \frac{1}{3}(q^2-1)(2q+1)/q^3$, and the probability that it has a triple root is $\tau = (q^2-1)/q^4$.*

2.2 Ternary cubic forms over $\mathbb{F}_q$.

We count the numbers of ternary cubic forms over $\mathbb{F}_q$, separating out all the different possible cases: smooth, irreducible but singular, or reducible in various ways.

We first count forms up to scaling by elements of $\mathbb{F}_q^\times$; these counts are then multiplied by $q-1$, and after adding 1 for the zero form, the counts for cubics add up to q^{10}.

2.2.1 Lines

The number of lines in $\mathbb{P}^2$ over $\mathbb{F}_{q^k}$ is $n_1^{(k)} = (q^{3k}-1)/(q^k-1)$. We write $n_1 = n_1^{(1)} = q^2+q+1$.

2.2.2 Conics

The total number of conics Q over $\mathbb{F}_q$ is $(q^6-1)/(q-1)$. Reducible conics are of three types, up to scaling: $Q = L^2$ with L a line over $\mathbb{F}_q$, or $Q = L_1L_2$ with lines L_j either both defined over $\mathbb{F}_q$ or conjugate over $\mathbb{F}_{q^2}$. The counts for these types are, up to scaling;

- $\#\{Q = L^2\} = n_1 = q^2+q+1$.
- $\#\{Q = L_1L_2 \text{ over } \mathbb{F}_q\} = n_1(n_1-1)/2 = \frac{1}{2}q(q+1)(q^2+q+1)$.
- $\#\{Q = L_1L_2 \text{ conjugate over } \mathbb{F}_{q^2}\} = (n_1^{(2)}-n_1)/2 = \frac{1}{2}q(q-1)(q^2+q+1)$.

Summing, we find that the number of absolutely reducible conics is $(q^2+1)(q^2+q+1)$. Hence the number of absolutely irreducible conics is $q^5-q^2 = q^2(q-1)(q^2+q+1)$, up to scaling.

2.2.3 Plane cubic curves

The number of plane cubic curves over $\mathbb{F}_q$, up to scaling, is $(q^{10}-1)/(q-1)$.

Reducible cubics are of the form $C = L^3$, $C = L_1^2 L_2$, or $C = L_1 L_2 L_3$ (with all lines L_j defined over $\mathbb{F}_q$) or $C = L_1 L_2 L_3$ (three lines conjugate over $\mathbb{F}_{q^3}$), or $C = L L_1 L_2$ (with L over $\mathbb{F}_q$ and L_1, L_2 conjugate over $\mathbb{F}_{q^2}$), or $C = LQ$ with Q an absolutely irreducible conic. The counts for these are, up to scaling:

- $\#\{C = L^3\} = n_1 = q^2+q+1$.
- $\#\{C = L_1 L_2^2\} = n_1(n_1-1) = q(q+1)(q^2+q+1)$.
- $\#\{C = L_1 L_2 L_3 \text{ over } \mathbb{F}_q\} = n_1(n_1-1)(n_1-2)/6 = \frac{1}{6}q(q+1)(q^2+q-1)(q^2+q+1)$.
- $\#\{C = L_1 L_2 L_3 \text{ conjugate over } \mathbb{F}_{q^3}\} = (n_1^{(3)} - n_1)/3 = \frac{1}{3}q(q^2-1)(q^3+q+1)$.

  Of these, we will later need to know the number that are concurrent (forming a "star") and the number that are not (forming a "triangle"), which are

  - (star) $\frac{1}{3}q(q^2-1)(q^2+q+1)$;
  - (triangle) $\frac{1}{3}q^3(q^2-1)(q-1)$.
- $\#\{C = L L_1 L_2 \text{ conjugate over } \mathbb{F}_{q^2}\} = n_1(n_1^{(2)} - n_1)/2 = \frac{1}{2}q(q-1)(q^2+q+1)^2$.
- $\#\{C = LQ\} = n_1(q^5-q^2) = q^2(q-1)(q^2+q+1)^2$.

Adding, we find that the number of absolutely reducible cubics is $(q+1)(q^6+q^5+q^4+q^2+1)$, and hence the number of absolutely irreducible cubics is

$$q^5(q+1)(q-1)(q^2+q+1) = Nq^2/(q-1)$$

where $N = |\mathrm{PGL}(3,\mathbb{F}_q)|$. Although it will not be needed for the proof of Theorem 1, we remark that Nq of these are smooth, with exactly N for each of the q possible j-invariants. Of the remaining cubics, N have a node and $N/(q-1)$ have a cusp.

3 Proof of Theorem 1

In this section, we prove Theorem 1 giving the density of plane cubic curves over $\mathbb{Q}_p$ that have a $\mathbb{Q}_p$-rational point.

3.1 Outline of the proof

Let C be a ternary cubic form with coefficients in $\mathbb{Z}_p$ that is *primitive*, meaning that not all of its coefficients are divisible by p. We say that C is *soluble* if there exist $x, y, z \in \mathbb{Q}_p$, not all zero, such that $C(x,y,z) = 0$, or in other words, if the associated cubic curve has a $\mathbb{Q}_p$-rational point.

The reduction of C modulo p is a cubic curve $\overline{C}$ over $\mathbb{F}_p$. If $\overline{C}$ has no $\mathbb{F}_p$-rational points then certainly C is not soluble. Since lines, smooth conics, and absolutely irreducible cubics over $\mathbb{F}_p$ always have smooth points, inspection of the cases enumerated in the previous section shows that $\overline{C}$ always

has smooth $\mathbb{F}_p$-points (even when $p = 2$) unless it is a product of three lines conjugate over $\mathbb{F}_{p^3}$ or a triple line; and in the former case, if the three lines are not concurrent then there are no $\mathbb{F}_p$-rational points at all.

It follows that C is not soluble when the reduction $\overline{C}$ consists of three non-concurrent lines conjugate over $\mathbb{F}_{p^3}$ (the *triangle* configuration); it may or may not be soluble when $\overline{C}$ is three concurrent lines conjugate over $\mathbb{F}_{p^3}$ (the *star* configuration) or a triple line; and in all other cases C is soluble. It remains to determine the density of soluble cubics whose reduction is either a star or a triple line. The density will not depend on which $\mathbb{F}_p$-rational point is the common point in the first case, or which $\mathbb{F}_p$-line is the triple line in the second, so in Sections 3.3 and 3.4 we take them to be $P_0 = [1 : 0 : 0]$ and $X = 0$, respectively. We will then develop recursions in order to solve for the densities of soluble cubics among those whose reductions lie in the star and triple line configurations.

3.2 Preliminaries

We now compute the probabilities of certain configurations occurring, including the ones already mentioned and two others which will arise in the course of the proof.

Let β_1 denote the probability of a ternary cubic over $\mathbb{Z}_p$ having a reduction which is a star as defined above, β_2 the probability of the reduction being a triple line, and β_3 the probability of the reduction being a triangle, again as defined above. Additionally, let β_4 be the probability of the *line condition*, defined to be the property that the reduction of the cubic meets the line $X = 0$ in three distinct points conjugate over $\mathbb{F}_{p^3}$, and let β_5 be the probability of the *point condition*, defined to be the property that the reduction of the cubic does not contain the point $P_0 = [1 : 0 : 0]$.

We will need to know the density of cubics over $\mathbb{Z}_p$ satisfying each of these conditions, as well as the relative density of those satisfying the star, triple line, and triangle conditions among those satisfying each of the line and point conditions. These relative densities will be denoted by β'_j and β''_j, respectively, for $j = 1, 2, 3$.

Proposition 7 *The probabilities of a random plane cubic over $\mathbb{F}_p$ satisfying each of these five conditions are as follows:*

1. *(star: all; relative to line condition; relative to point condition)*

$$\beta_1 = \frac{(p^2-1)(p^3-1)}{3p^9}; \qquad \beta'_1 = \frac{1}{p^4}; \qquad \beta''_1 = \frac{(p+1)^2(p-1)}{3p^7};$$

2. *(triple line: all; relative to line condition; relative to point condition)*

$$\beta_2 = \frac{p^3-1}{p^{10}}; \qquad \beta'_2 = 0; \qquad \beta''_2 = \frac{1}{p^7};$$

3. *(triangle: all; relative to line condition; relative to point condition)*

$$\beta_3 = \frac{(p+1)(p-1)^3}{3p^7}; \qquad \beta'_3 = \frac{p-1}{p^4}; \qquad \beta''_3 = \frac{(p+1)(p-1)^2}{3p^6};$$

4. *(line condition)*

$$\beta_4 = \frac{(p+1)(p-1)^2}{3p^3};$$

5. *(point condition)*

$$\beta_5 = \frac{p-1}{p}.$$

Proof: We refer to the previous section for the numbers of stars, triple lines and triangles, up to scaling. Multiplying by $(p-1)/p^{10}$ gives β_j for $j = 1, 2, 3$.

1. The probability of satisfying the star condition centred at a given point in $\mathbb{P}^2(\mathbb{F}_p)$ is

$$\gamma = \frac{1}{3}p(p^2-1) \cdot \frac{p-1}{p^{10}}.$$

   We have already computed $\beta_1 = (p^2+p+1)\gamma$. The probability of satisfying both the line and star condition is $p^2\gamma$. Dividing by β_4 gives β_1'. Similarly, the probability of satisfying both the point and star condition is $(p^2+p)\gamma$ which on dividing by β_5 gives β_1''.

2. The triple line and line conditions cannot occur together, so $\beta_2' = 0$. The triple line and point conditions together have probability $p^2(p-1)/p^{10}$, and dividing by β_5 gives β_2''.

3. Since the triangle condition implies both the line and point conditions, $\beta_3' = \beta_3/\beta_4 = (p-1)/p^4$, and $\beta_3'' = \beta_3/\beta_5 = (p+1)(p-1)^2/3p^6$.

4. The line condition holds with the same probability that a binary cubic form over $\mathbb{Z}_p$ is irreducible modulo p, which by Lemma 5 is

$$\beta_4 = \frac{1}{3}p(p^2-1) \cdot \frac{p-1}{p^4}.$$

5. The point condition is equivalent to the condition that the coefficient of X^3 in the cubic form is not divisible by p, so occurs with probability $\beta_5 = 1 - 1/p$.

□

For $1 \leq j \leq 5$, let α_j denote the probability of solubility for ternary cubics whose reduction is a star, a triple line, a triangle, or which satisfy the line or point conditions, respectively. We know that $\alpha_3 = 0$. In the next two subsections, we compute α_1, α_4, α_2, and α_5.

3.3 The star case: computation of α_1 (together with α_4)

We derive two linear equations linking α_1 and α_4, from which their values may be determined.

Lemma 8 $1 - \alpha_4 = \beta_1'(1-\alpha_1) + \beta_2'(1-\alpha_2) + \beta_3'$. *Hence* $\alpha_4 = (p^4 - p + \alpha_1)/p^4$.

Proof: For the first equation, we combine the probablities of insolubility in the star, triple line, and triangle cases, the latter being 1. Using the values of β_j' from Proposition 7 allows us to solve for α_4 in terms of α_1 alone, since the coefficient of α_2 is conveniently $\beta_2' = 0$. □

We write $v(f)$ for the valuation of a form f with coefficients in $\mathbb{Z}_p$, that is, the minimum of the valuations of the coefficients.

Lemma 9 $\alpha_1 = (p^3 - p + \alpha_4)/p^4$.

Proof: Without loss of generality the centre of the star is at $P_0 = [1 : 0 : 0]$, so the cubic has the form

$$C = c_0X^3 + c_1(Y, Z)X^2 + c_2(Y, Z)X + c_3(Y, Z)$$

where each c_j is a binary form of degree j and the valuations of c_0, c_1, c_2, c_3 satisfy

$$\geq 1 \qquad \geq 1 \qquad \geq 1 \qquad = 0$$

respectively, with c_3 irreducible modulo p. Solubility of C means that there exist $x, y, z \in \mathbb{Z}_p$, not all in $p\mathbb{Z}_p$, satisfying $C(x, y, z) = 0$. Here, for any such solution, irreducibility of c_3 modulo p implies that $y, z \equiv 0 \pmod{p}$.

If $v(c_0) = 1$ (which has probability $1 - 1/p$), then C is insoluble since the first term has valuation 1 while the other terms have valuation at least 2. So we may assume that $v(c_0) \geq 2$ (which has probability $1/p$), substitute pY, pZ for Y, Z, and divide by p^2. The valuations of the binary forms now satisfy

$$\geq 0 \qquad \geq 0 \qquad \geq 1 \qquad = 1.$$

If $v(c_1) = 0$ (which has probability $1 - 1/p^2$ since c_1 has two coefficients), then $C \pmod{p}$ has a simple linear factor over $\mathbb{F}_p$ and hence is soluble. Otherwise, we have $v(c_1) \geq 1$ (which has probability $1/p^2$), and the valuations of the binary forms satisfy

$$\geq 0 \qquad \geq 1 \qquad \geq 1 \qquad = 1.$$

We must have $x \not\equiv 0 \pmod{p}$ by primitivity, since we have already forced $y \equiv z \equiv 0$ (in the original coordinates). Hence for solubility we must have $c_0 \equiv 0 \pmod{p}$; that is, $v(c_0) \geq 1$. Assuming this, which has probability $1/p$, we may divide through by p to obtain valuations satisfying

$$\geq 0 \qquad \geq 0 \qquad \geq 0 \qquad = 0.$$

Recalling that c_3 is irreducible modulo p, we see that this is an arbitrary cubic satisfying the line condition, so the probability of solubility is α_4.

Tracing through the above steps, we see that

$$\alpha_1 = (1 - 1/p) \cdot 0 + (1/p) \cdot \left((1 - 1/p^2) \cdot 1 + (1/p^2) \cdot ((1 - 1/p) \cdot 0 + (1/p) \cdot \alpha_4)\right),$$

which simplifies to the equation stated. □

Solving for α_1 now gives

Proposition 10

$$\alpha_1 = \frac{p^7 - p^5 + p^4 - p}{p^8 - 1} = \frac{p(p-1)(p^5 + p^4 + p^2 + p + 1)}{p^8 - 1}.$$

3.4 The triple line case: computation of α_2 (together with α_5)

Recall that α_2 and α_5 denote the probabilities of solubility given the triple line and point conditions, respectively. We derive two equations linking these quantities (and α_1), from which they may be determined.

First, we have the analogue of Lemma 8:

Lemma 11 $1 - \alpha_5 = \beta_1''(1 - \alpha_1) + \beta_2''(1 - \alpha_2) + \beta_3''$.

To obtain a second equation between α_2 and α_5, we first need to determine the probability of solubility given a refinement of the triple line configuration. For $j = 1, 2$, let ν_j denote the probability of solubility for cubics C whose reduction is the triple line $Y = 0$ and that also satisfy the condition that the coefficient of X^3 has valuation exactly j and the coefficients of X^2Y, X^2Z have valuations at least j (in earlier notation: c_3 has a triple root modulo p, $v(c_0) = j$, $v(c_1) \geq j$, and $v(c_2) \geq 1$).

Lemma 12

$$\nu_1 = \frac{2p^8 + p^6 - 3p^5 + 3p^4 - p^2 - 2}{3(p^8 - 1)}; \qquad \nu_2 = \frac{3p^8 - 3p^7 + 3p^6 - p^4 - 2}{3(p^8 - 1)}.$$

Proof: Let σ_1 and τ_1 denote the probabilities that a monic cubic polynomial over $\mathbb{F}_p$ has a simple root over $\mathbb{F}_p$, or a triple root, respectively, as in Corollary 4.

We arrange the 10 coefficients of the ternary cubic form C in a triangle with the Z^3-coefficient at the top, the X^3-coefficient at bottom left and Y^3-coefficient at bottom right, and indicate their valuations using the same equality/inequality notation as before. The condition on a member C in the set of cubics considered in the definition of ν_1 is then expressed by

$$\begin{array}{cccccc} Z^3 & \geq 1 & & & & \\ & \geq 1 & \geq 1 & & & \\ & \geq 1 & \geq 1 & \geq 1 & & \\ X^3 & = 1 & \geq 1 & \geq 1 & = 0 & Y^3 \end{array}$$

Any solution must have $y \equiv 0 \pmod{p}$, so we substitute pY for Y and divide by p to obtain

$$\begin{array}{cccccc} Z^3 & \geq 0 & & & & \\ & \geq 0 & \geq 1 & & & \\ & \geq 0 & \geq 1 & \geq 2 & & \\ X^3 & = 0 & \geq 1 & \geq 2 & = 2 & Y^3 \end{array}$$

Now the reduction is a binary cubic in X, Z with unit X^3 coefficient. If it has a simple root in $\mathbb{F}_p$ (probability σ_1), it lifts to a p-adic root and C is soluble with $y = 0$. Otherwise, C is insoluble unless there is a triple root (probability τ_1), since otherwise we could force $x \equiv z \equiv 0 \pmod{p}$. Given a triple root, we can shift the root to 0, so that the binary cubic is a constant times X^3. Now the valuations are

$$\begin{array}{cccccc} Z^3 & \geq 1 & & & & \\ & \geq 1 & \geq 1 & & & \\ & \geq 1 & \geq 1 & \geq 2 & & \\ X^3 & = 0 & \geq 1 & \geq 2 & = 2 & Y^3 \end{array}$$

The probability of solubility in this case is ν_2. Tracing through the arguments so far we have $\nu_1 = \sigma_1 + \tau_1\nu_2$. We replace X by pX and divide through by p:

$$\begin{array}{lllll} Z^3 & \geq 0 & & & \\ & \geq 1 & \geq 0 & & \\ & \geq 2 & \geq 1 & \geq 1 & \\ X^3 & = 2 & \geq 2 & = 1 & Y^3 \end{array}$$

If the coefficient of YZ^2 has valuation 0 (with probability $1-1/p$), then the reduction is a binary cubic in Y, Z with a simple root, so C is soluble. Otherwise, C reduces to a multiple of Z^3, but since $z \equiv 0 \pmod{p}$ is not allowed, solubility requires that the coefficient of Z^3 also has valuation at least 1. So we have insolubility with probability $1/p - 1/p^2$ and otherwise we can divide through by p to obtain

$$\begin{array}{lllll} Z^3 & \geq 0 & & & \\ & \geq 0 & \geq 0 & & \\ & \geq 1 & \geq 0 & \geq 0 & \\ X^3 & = 1 & \geq 1 & = 0 & Y^3 \end{array}$$

If the coefficients of XYZ and XZ^2 are not both zero modulo p (probability $1 - 1/p^2$), then we have solubility since the reduction is either absolutely irreducible or has a simple linear factor over $\mathbb{F}_p$. Otherwise (probability $1/p^2$) we have

$$\begin{array}{lllll} Z^3 & \geq 0 & & & \\ & \geq 1 & \geq 0 & & \\ & \geq 1 & \geq 1 & \geq 0 & \\ X^3 & = 1 & \geq 1 & = 0 & Y^3 \end{array}$$

where the reduction is a binary cubic in Y, Z with unit Y^3 coefficient. We have solubility if it has a simple $\mathbb{F}_p$-root (probability σ_1), otherwise insolubility unless it has a triple root (probability τ_1), in which case the valuations are exactly as at the start, where solubility has probability ν_1.

Tracing through the above, we see that

$$\nu_2 = (1-1/p)\cdot 1 + (1/p^2)\cdot\big((1-1/p^2)\cdot 1 + (1/p^2)\cdot(\sigma_1 + \tau_1\nu_1)\big).$$

Recalling that $\nu_1 = \sigma_1 + \tau_1\nu_2$, we may now solve for both ν_1 and ν_2. □

The second equation linking α_5 and α_2 will involve the above quantities ν_1 and ν_2, and uses an argument similar to the one used in the star case. Let σ and τ denote the probabilities that a binary cubic over $\mathbb{F}_p$ has a simple root over $\mathbb{F}_p$ or a triple root, respectively, as in Corollary 6.

Lemma 13 $\alpha_2 = \sigma + \tau\nu_2 + (1/p^4)\big((1-1/p^3) + (1/p^3)(\sigma + \tau\nu_1 + (1/p^4)\alpha_5)\big)$.

Proof: We may assume that the triple line modulo p is $X = 0$. Using the same notation as before, let us write

$$C = c_0X^3 + c_1(Y,Z)X^2 + c_2(Y,Z)X + c_3(Y,Z)$$

where each c_j is a binary form of degree j; then the valuations of the c_j satisfy

$$= 0 \qquad \geq 1 \qquad \geq 1 \qquad \geq 1.$$

Solutions must have $x \equiv 0 \pmod{p}$ so we replace X by pX and divide by p to obtain

$$= 2 \qquad \geq 2 \qquad \geq 1 \qquad \geq 0,$$

so that C reduces to a binary cubic in Y, Z.

With probability σ this binary cubic has a simple $\mathbb{F}_p$-root and C is soluble. With probability τ it has a triple root (without loss of generality the reduction is Z^3); in this case, C is soluble with probability ν_2. Otherwise, for solubility we require $v(c_3) \geq 1$, as otherwise solutions would have $y \equiv z \equiv 0 \pmod{p}$, which is not allowed since we have already scaled X. So with probability $1/p^4$ we have the valuations satisfying

$$= 2 \qquad \geq 2 \qquad \geq 1 \qquad \geq 1$$

and dividing through by p we obtain

$$= 1 \qquad \geq 1 \qquad \geq 0 \qquad \geq 0.$$

Now, with probability $1 - 1/p^3$ we have $v(c_2) = 0$ and solubility since the reduction is either absolutely irreducible or has a simple linear factor over $\mathbb{F}_p$. Otherwise (probability $1/p^3$), we have $v(c_2) \geq 1$:

$$= 1 \qquad \geq 1 \qquad \geq 1 \qquad \geq 0.$$

As at the start, we have solubility if c_3 has a simple $\mathbb{F}_p$-root (probability σ), solubility with probability ν_1 if it has a triple root (probability τ), and otherwise for solubility we require $v(c_3) \geq 1$ (probability $1/p^4$) in which case we divide through by p. The latter gives an arbitrary cubic subject to the point condition, where the probability of solubility is α_5.

Tracing through the above steps, we see that

$$\alpha_2 = \sigma \cdot 1 + \tau\nu_2 + (1/p^4)\left((1 - 1/p^3) \cdot 1 + (1/p^3) \cdot (\sigma \cdot 1 + \tau\nu_1 + (1/p^4)\alpha_5)\right),$$

which is the equation stated. □

Using the equations given in Lemmas 11 and 13, together with the known value of α_1, we can solve for α_2, obtaining the following.

Proposition 14

$$\alpha_2 = 1 - \frac{p^{14} + 3p^{11} + p^8 + 2p^7 + p^5 + p^4 + 1}{3(p^2+1)(p^2+p+1)(p^4+1)(p^6+p^3+1)}.$$

3.5 Conclusion

The probability of insolubility of a ternary cubic with coefficients in $\mathbb{Q}_p$ is therefore

$$\begin{aligned} 1 - \rho(p) &= \frac{p^{10}}{p^{10}-1}(\beta_1(1-\alpha_1) + \beta_2(1-\alpha_2) + \beta_3) \\ &= f(p)/g(p), \end{aligned}$$

where f and g are the polynomials given in the statement of Theorem 1.

4 The probability that a random plane cubic over $\mathbb{Q}_p$ has points over the maximal unramified extension of $\mathbb{Q}_p$

Let $\mathbb{Q}_p^{\mathrm{nr}}$ denote the maximal unramified extension of $\mathbb{Q}_p$.

Theorem 15 *The probability that a random plane cubic curve over $\mathbb{Q}_p$ has a $\mathbb{Q}_p^{\mathrm{nr}}$-rational point is given by*

$$\rho^{\mathrm{nr}}(p) = 1 - \frac{p^{11}(p-1)(p^2-1)(p^3-1)}{(p^8-1)(p^9-1)(p^{10}-1)}.$$

Note that the formula for the probability in Theorem 15 is much simpler than that in Theorem 1.

The proof of Theorem 1 may be regarded as an algorithm for testing whether a plane cubic is locally soluble (i.e., has a $\mathbb{Q}_p$-point), where we are able to determine explicitly the probability of entering each step of the algorithm. The algorithm terminates either when there is a smooth $\mathbb{F}_p$-point on the reduction (in which case it lifts to a $\mathbb{Q}_p$-point by Hensel's lemma) or when we reach one of the following four situations:

($\mathbf{I}_{3m}$) The reduction $\overline{C}$ consists of three non-concurrent lines conjugate over $\mathbb{F}_{p^3}$ (the triangle configuration).

(IV) The cubic is $\mathrm{GL}_3(\mathbb{Z}_p)$-equivalent to a cubic of the form

$$C = c_0X^3 + c_1(Y,Z)X^2 + c_2(Y,Z)X + c_3(Y,Z)$$

where each c_j is a binary form of degree j and the valuations of the c_j satisfy

$$= 1 \qquad \geq 1 \qquad \geq 1 \qquad = 0$$

with c_3 irreducible modulo p.

(IV*) As in (IV), except that the valuations satisfy

$$= 2 \qquad \geq 2 \qquad \geq 1 \qquad = 0.$$

(Cr) The cubic is $\mathrm{GL}_3(\mathbb{Z}_p)$-equivalent to a cubic C whose coefficients have valuations satisfying

$$\begin{array}{cccccc} Z^3 & = 2 & & & & \\ & \geq 2 & \geq 2 & & & \\ & \geq 1 & \geq 1 & \geq 2 & & \\ X^3 & = 0 & \geq 1 & \geq 1 & = 1 & Y^3 \end{array}$$

In the first three cases the cubic is insoluble over $\mathbb{Q}_p$ but soluble over $\mathbb{Q}_p^{\mathrm{nr}}$; it can be shown that the Jacobian is an elliptic curve $E/\mathbb{Q}_p$ with Kodaira symbol I_{3m}, IV, or IV* as indicated, and Tamagawa number divisible by 3. In the final case, the cubic is a critical model, in the terminology of [5, Definition 5.1]. As noted in [5], critical models are insoluble over $\mathbb{Q}_p^{\mathrm{nr}}$.

The probability that a cubic is insoluble over $\mathbb{Q}_p$, denoted $f(p)/g(p)$ in Theorem 1, may thus be written as a sum of four terms, corresponding to the four situations above. This allows us to naturally adapt the proof of Theorem 1 to a proof also of Theorem 15.

Proof of Theorem 15: Since the proof of Theorem 15 is similar to that of Theorem 1, we only highlight the differences. Let α_1', α_2', ν_1', ν_2' be the probabilities of insolubility over $\mathbb{Q}_p^{\mathrm{nr}}$, in the situations where we earlier wrote α_1, α_2, ν_1, ν_2 for the probabilities of solubility over $\mathbb{Q}_p$. The analogue of Lemma 12 gives

$$\nu_1' \;=\; \frac{p^4(p-1)}{p^8-1}, \qquad \nu_2' \;=\; \frac{p^6(p-1)}{p^8-1}.$$

We have $\alpha_1' = 0$. The analogues of Lemmas 11 and 13 give

$$\alpha_2' \;=\; \tau\nu_2' + \frac{1}{p^7}\left(\tau\nu_1' + \frac{1}{p^4}\beta_2''\alpha_2'\right).$$

Substituting $\nu_1' = \nu_2'/p^2$ and solving for α_2' gives

$$\alpha_2' \;=\; \frac{p^5(p^2-1)}{p^9-1}\nu_2' \;=\; \frac{p^{11}(p-1)(p^2-1)}{(p^8-1)(p^9-1)}.$$

Finally, the probability of insolubility over $\mathbb{Q}_p^{\mathrm{nr}}$ is

$$\frac{p^{10}}{p^{10}-1}\beta_2\alpha_2' \;=\; \frac{p^{11}(p-1)(p^2-1)(p^3-1)}{(p^8-1)(p^9-1)(p^{10}-1)}.$$

□

By the same argument as in [11], we see that Theorem 15 implies that the probability ρ^{nr} that a random plane cubic curve over $\mathbb{Q}$ has a point over $\mathbb{Q}_p^{\mathrm{nr}}$ for all primes p is given by

$$\rho^{\mathrm{nr}} = \prod_p \rho^{\mathrm{nr}}(p) = \prod_p \left(1 - \frac{p^{11}(p-1)(p^2-1)(p^3-1)}{(p^8-1)(p^9-1)(p^{10}-1)}\right) \approx 99.96676\%.$$

By [5, Thm. 3.5], this may be interpreted as the probability that a plane cubic curve over $\mathbb{Q}$ has minimal discriminant the same as that of its Jacobian elliptic curve.

5 Concluding remarks and further questions

We have shown that the density ρ of locally soluble plane cubics over $\mathbb{Z}$ is equal to $\prod_p \rho(p)$, where $\rho(p)$, the density of plane cubics over $\mathbb{Z}_p$ that have a $\mathbb{Q}_p$-point, is a fixed rational function of p *independent of* p. We have also proven analogously that the density ρ^{nr} of plane cubics over $\mathbb{Z}$ having a point locally over $\mathbb{Q}_p^{\mathrm{nr}}$ for all p is given by $\prod_p \rho^{\mathrm{nr}}(p)$, where $\rho^{\mathrm{nr}}(p)$, the density of plane cubics over $\mathbb{Z}_p$ that have a $\mathbb{Q}_p^{\mathrm{nr}}$-point, is again a fixed rational function of p independent of p. We determined these rational functions $\rho(p)$ and $\rho^{\mathrm{nr}}(p)$ explicitly in Theorems 1 and 15.

It follows from the work of Denef and Loeser [6] that quantities such as $\rho(p)$ (and perhaps, with some work, also $\rho^{\mathrm{nr}}(p)$) can be expressed in terms of rational functions of the counts of $\mathbb{F}_p$-points on a finite number of $\mathbb{Z}$-schemes. But it is only in special situations (such as in the results we have obtained here) that the answer is a fixed rational function of p, although we know of no results in the literature from which this could be deduced *a priori*. It is an interesting problem to determine general sufficient conditions for when $\mathbb{F}_p$-counts on a $\mathbb{Z}$-scheme (or for local solubility densities $\rho_S(p)$ for spaces of forms S over $\mathbb{Z}$) are fixed rational functions of p. For some interesting varieties with polynomial counts (mod p) for all p or at least for "many p" (e.g., for Chebotarev sets of p) see, e.g., [9, Appendix], [12], and [10].

Acknowledgments

We are very grateful to Bhargav Bhatt, François Loeser, Bjorn Poonen, Michael Stoll, and Damiano Testa for helpful conversations. The first author was supported by a Simons Investigator Grant and NSF grant DMS-1001828. The second author was supported by EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms.

References

[1] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, http://arxiv.org/abs/1402.1131.

[2] M. Bhargava, The Ekedahl sieve and the density of squarefree values of invariant polynomials, http://arxiv.org/abs/1402.0031.

[3] M. Bhargava, J. Cremona, and T. A. Fisher, N. G. Jones, and J. P. Keating, What is the probability that a random integral quadratic form in n variables has an integral zero?, http://arxiv.org/abs/1502.05992

[4] M. Bhargava, J. Cremona, and T. A. Fisher, The density of hyperelliptic curves over $\mathbb{Q}$ of genus g that have a point everywhere locally, preprint.

[5] J. Cremona, T. A. Fisher, and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, *Alg. & Num. Th.* **4**, No. 6 (2010), 763–820.

[6] J. Denef and F. Loeser, Definable sets, motives and p-adic integrals, *J. Amer. Math. Soc.* **14** (2001), 429–469.

[7] T. Ekedahl, An infinite version of the Chinese remainder theorem, *Comment. Math. Univ. St. Paul.* **40** (1991), 53–59.

[8] T. A. Fisher and G. F. Sills, Local solubility and height bounds for coverings of elliptic curves, *Math. Comp.* **81** (2012), no. 279, 1635–1662.

[9] T. Hausel and F. Rodriguez-Villegas (with an Appendix by N. M. Katz), Mixed Hodge polynomials of character varieties, *Invent. Math.* **174** (2008), no. 3, 555–624.

[10] M. Kisin and G. Lehrer, Eigenvalues of Frobenius and Hodge numbers, *Quart. J. Pure and Appl. Math.* **2** (2006), no. 2, issue in honour of John Coates, 497–518.

[11] B. Poonen and P. Voloch, Random Diophantine equations, *Arithmetic of Higher-Dimensional Algebraic Varieties*, 175–184, *Progress in Mathematics* **226**, 2004, Birkhäuser, Boston, MA.

[12] T. van den Bogaart and B. Edixhoven, Algebraic stacks whose number of points over finite fields is a polynomial, *Number Fields and Function Fields- Two Parallel Worlds*, Progress in Mathematics **239**, G. van der Geer, B. Moonen, and R. Schoof (Eds.), 2005.