Some density results in number theory

John Cremona

University of Warwick

—

with Manjul Bhargava (Princeton) and Tom Fisher (Cambridge)

Coates birthday conference, Cambridge, 25 March 2015

EPSRC
Engineering and Physical Sciences
Research Council

THE UNIVERSITY OF WARWICK

Overview

1. Introduction
2. Description of three classes of equations to be discussed
3. Remarks on distributions and random sampling
4. Statement of results A: quadrics
5. Statement of results B: cubics
6. Statement of results C: quartics

Overview

1. Introduction
2. Description of three classes of equations to be discussed
3. Remarks on distributions and random sampling
4. Statement of results A: quadrics
5. Statement of results B: cubics
6. Statement of results C: quartics

See (A) `http://arxiv.org/abs/1502.05992`
and (B) `http://arxiv.org/abs/1311.5578`.

Introduction

I will discuss a number of results in number theory (Diophantine equations or Diophantine geometry) all of the form

> *"What is the probability that a random equation of the form . . . has a solution?"*

Introduction

I will discuss a number of results in number theory (Diophantine equations or Diophantine geometry) all of the form

> *"What is the probability that a random equation of the form . . . has a solution?"*

I will of course be more precise what I mean by

- *equation* (there will be three families), by
- *probability* and *random*, and by
- *solution*.

Introduction

I will discuss a number of results in number theory (Diophantine equations or Diophantine geometry) all of the form

> *"What is the probability that a random equation of the form ... has a solution?"*

I will of course be more precise what I mean by

- *equation* (there will be three families), by
- *probability* and *random*, and by
- *solution*.

All equations will be (possibly weighted) homogeneous, and we will consider *local solubility* (over $\mathbb{R}$ or $\mathbb{Q}_p$) as well as *global solubility* (over $\mathbb{Q}$) or in some cases *everywhere local solubility* (over all completions of $\mathbb{Q}$).

Equations A: quadrics in n variables

We consider quadratic forms $Q(X_1, \ldots, X_n)$ in n variables ("n-ary quadrics")

$$Q = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j$$

given by $N = n(n+1)/2$ homogeneous coefficients a_{ij} in a field K, and seek solutions (zeros) in $\mathbb{P}^{n-1}$. We call Q *isotropic over* K if there is a solution in $\mathbb{P}^{n-1}(K)$.

Equations A: quadrics in n variables

We consider quadratic forms $Q(X_1, \ldots, X_n)$ in n variables ("n-ary quadrics")

$$Q = \sum_{1 \leq i \leq j \leq n} a_{ij} X_i X_j$$

given by $N = n(n+1)/2$ homogeneous coefficients a_{ij} in a field K, and seek solutions (zeros) in $\mathbb{P}^{n-1}$. We call Q *isotropic over* K if there is a solution in $\mathbb{P}^{n-1}(K)$.

We will consider this for $K = \mathbb{R}$, for $K = \mathbb{Q}_p$ (where we may assume $a_{ij} \in \mathbb{Z}_p$ by homogeneity) and for $K = \mathbb{Q}$ (with $a_{ij} \in \mathbb{Z}$), recalling that the Hasse principle holds for quadrics.

Equations B: ternary cubics

Here we consider ternary cubic forms $f(X,Y,Z)$ with 10 coefficients in K, and seek solutions (zeros) in $\mathbb{P}^2(K)$.

Equations B: ternary cubics

Here we consider ternary cubic forms $f(X,Y,Z)$ with 10 coefficients in K, and seek solutions (zeros) in $\mathbb{P}^2(K)$.

Again, by homogeneity when $K=\mathbb{Q}$ or $K=\mathbb{Q}_p$ we may assume that the coefficients are integral.

Equations B: ternary cubics

Here we consider ternary cubic forms $f(X,Y,Z)$ with 10 coefficients in K, and seek solutions (zeros) in $\mathbb{P}^2(K)$.

Again, by homogeneity when $K=\mathbb{Q}$ or $K=\mathbb{Q}_p$ we may assume that the coefficients are integral.

Since there is no Hasse principle for plane cubics, over $\mathbb{Q}$ we will only ask for everywhere local solubility. As solubility over $\mathbb{R}$ is obviously automatic, this amounts to solubility over $\mathbb{Q}_p$ for all primes p.

Equations C: elliptic quartics

We consider quartic (hyper)elliptic equations $Z^2 = f(X, Y)$ with f a binary form of degree 4 over K, defined by 5 coefficients.

Equations C: elliptic quartics

We consider quartic (hyper)elliptic equations $Z^2 = f(X, Y)$ with f a binary form of degree 4 over K, defined by 5 coefficients.

Again, over $\mathbb{Q}$ we only ask for everywhere local solubility; solubility over $\mathbb{R}$ is now a non-trivial question.

Equations C: elliptic quartics

We consider quartic (hyper)elliptic equations $Z^2 = f(X, Y)$ with f a binary form of degree 4 over K, defined by 5 coefficients.

Again, over $\mathbb{Q}$ we only ask for everywhere local solubility; solubility over $\mathbb{R}$ is now a non-trivial question.

We could more generally consider hyperelliptic curves of higher genus, defined by similar equations for $\deg(f) = 2g + 2$; the odd degree case is trivial since then the unique point at infinity is K-rational. So far we have only partial results for $g > 1$, which we will mention briefly towards the end.

Local questions A: quadrics in n variables

(p) Local question at p: if the coefficients $a_{ij} \in \mathbb{Z}_p$ are chosen at random, what is the probability that Q is isotropic over $\mathbb{Q}_p$?

Local questions A: quadrics in n variables

(p) Local question at p: if the coefficients $a_{ij} \in \mathbb{Z}_p$ are chosen at random, what is the probability that Q is isotropic over $\mathbb{Q}_p$? More precisely, what the the p-adic measure $\rho_n(p)$ of the subset

$$\{(a_{ij}) \in \mathbb{Z}_p^N \mid Q \text{ isotropic}/\mathbb{Q}_p\} \subseteq \mathbb{Z}_p^N$$

(or the density of soluble quadrics, since $\mathbb{Z}_p$ has measure 1)?

Local questions A: quadrics in n variables

(p) Local question at p: if the coefficients $a_{ij} \in \mathbb{Z}_p$ are chosen at random, what is the probability that Q is isotropic over $\mathbb{Q}_p$?
More precisely, what the the p-adic measure $\rho_n(p)$ of the subset

$$\{(a_{ij}) \in \mathbb{Z}_p^N \mid Q \text{ isotropic}/\mathbb{Q}_p\} \subseteq \mathbb{Z}_p^N$$

(or the density of soluble quadrics, since $\mathbb{Z}_p$ has measure 1)?
We give an exact formula for $\rho_n(p)$.

Local questions A: quadrics in n variables

(p) Local question at p: if the coefficients $a_{ij} \in \mathbb{Z}_p$ are chosen at random, what is the probability that Q is isotropic over $\mathbb{Q}_p$? More precisely, what the the p-adic measure $\rho_n(p)$ of the subset

$$\{(a_{ij}) \in \mathbb{Z}_p^N \mid Q \text{ isotropic}/\mathbb{Q}_p\} \subseteq \mathbb{Z}_p^N$$

(or the density of soluble quadrics, since $\mathbb{Z}_p$ has measure 1)? We give an exact formula for $\rho_n(p)$.

(∞) Local question over $\mathbb{R}$: let D be a “nice” distribution on $\mathbb{R}^N$, that is, a piecewise smooth rapidly decaying function whose integral over $\mathbb{R}^N$ is 1. What is

$$\rho_n^D(\infty) = \int_{Q \in \mathbb{R}^N, \text{isotropic}/\mathbb{R}} D(Q) dQ?$$

Which real distributions for quadrics?

We will consider two distributions: the uniform distribution (U) on $[-\frac{1}{2}, \frac{1}{2}]^N$, and the Gaussian Orthogonal Ensemble (GOE):

Which real distributions for quadrics?

We will consider two distributions: the uniform distribution (U) on $[-\frac{1}{2}, \frac{1}{2}]^N$, and the Gaussian Orthogonal Ensemble (GOE): in the GOE, $(a_{ij}) = \frac{1}{\sqrt{2}}(M + M^t)$ where the n^2 entries of M are i.i.d. Gaussians.

Which real distributions for quadrics?

We will consider two distributions: the uniform distribution (U) on $[-\frac{1}{2}, \frac{1}{2}]^N$, and the Gaussian Orthogonal Ensemble (GOE): in the GOE, $(a_{ij}) = \frac{1}{\sqrt{2}}(M + M^t)$ where the n^2 entries of M are i.i.d. Gaussians.
We can evaluate $\rho_n^{GOE}(\infty)$ exactly, but only have numerical approximations for $\rho_n^U(\infty)$.

Global questions A: quadrics in n variables

We will make precise what we mean by taking a random *integral* quadratic form with respect to some distribution D on $\mathbb{R}^N$, and asking for the probability that it is isotropic over $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$.

Global questions A: quadrics in n variables

We will make precise what we mean by taking a random *integral* quadratic form with respect to some distribution D on $\mathbb{R}^N$, and asking for the probability that it is isotropic over $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$.

By the Hasse-Minkowski theorem we expect that the global probability is the product for the local ones, but this needs to be stated and proved carefully!

Global questions A: quadrics in n variables

We will make precise what we mean by taking a random *integral* quadratic form with respect to some distribution D on $\mathbb{R}^N$, and asking for the probability that it is isotropic over $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{Q}_p$.

By the Hasse-Minkowski theorem we expect that the global probability is the product for the local ones, but this needs to be stated and proved carefully!

For $K = \mathbb{R}$, $\mathbb{Q}$ or $\mathbb{Q}_p$ define

$$\rho_n^D(K) = \lim_{X \to \infty} \frac{\sum_{Q \in \mathbb{Z}^N \text{ isotropic}/K} D(Q/X)}{\sum_{Q \in \mathbb{Z}^N} D(Q/X)}.$$

Results A: quadrics in n variables (1)

Theorem (A0)

$\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$, *and* $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ *(independent of* D*).*

Results A: quadrics in n variables (1)

Theorem (A0)

$\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$, and $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ (independent of D).

In words: the probability that a D-random integral quadratic form is isotropic over $\mathbb{R}$ is the same as the probability that a D-random real quadratic form is isotropic.

Results A: quadrics in n variables (1)

Theorem (A0)

$\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$, and $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ (independent of D).

In words: the probability that a D-random integral quadratic form is isotropic over $\mathbb{R}$ is the same as the probability that a D-random real quadratic form is isotropic.

Similarly, the probability that a D-random integral quadratic form is isotropic over $\mathbb{Q}_p$ is the same as the probability that a random quadratic form over $\mathbb{Z}_p$ (with respect to the p-adic measure on $\mathbb{Z}_p^N$) is isotropic over $\mathbb{Q}_p$.

Results A: quadrics in n variables (1)

Theorem (A0)

$\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$, and $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ (independent of D).

In words: the probability that a D-random integral quadratic form is isotropic over $\mathbb{R}$ is the same as the probability that a D-random real quadratic form is isotropic.

Similarly, the probability that a D-random integral quadratic form is isotropic over $\mathbb{Q}_p$ is the same as the probability that a random quadratic form over $\mathbb{Z}_p$ (with respect to the p-adic measure on $\mathbb{Z}_p^N$) is isotropic over $\mathbb{Q}_p$.

Theorem (A1)

$\rho_n^D(\mathbb{Q}) = \rho_n^D(\infty) \prod_p \rho_n(p) = \rho_n^D(\mathbb{R}) \prod_p \rho_n^D(\mathbb{Q}_p)$.

Results A: quadrics in n variables (1)

Theorem (A0)

$\rho_n^D(\mathbb{R}) = \rho_n^D(\infty)$, and $\rho_n^D(\mathbb{Q}_p) = \rho_n(p)$ (independent of D).

In words: the probability that a D-random integral quadratic form is isotropic over $\mathbb{R}$ is the same as the probability that a D-random real quadratic form is isotropic.

Similarly, the probability that a D-random integral quadratic form is isotropic over $\mathbb{Q}_p$ is the same as the probability that a random quadratic form over $\mathbb{Z}_p$ (with respect to the p-adic measure on $\mathbb{Z}_p^N$) is isotropic over $\mathbb{Q}_p$.

Theorem (A1)

$\rho_n^D(\mathbb{Q}) = \rho_n^D(\infty)\prod_p \rho_n(p) = \rho_n^D(\mathbb{R})\prod_p \rho_n^D(\mathbb{Q}_p)$.

For $D = U$ this follows from a result of Poonen and Voloch.

Results A: quadrics in n variables (2)

Theorem (A2)

The probability $\rho_n(p)$ that a random n-ary quadric over $\mathbb{Z}_p$ is isotropic over $\mathbb{Q}_p$ is

n	$\rho_n(p)$
1	0
2	$1/2$
3	$1 - \frac{p}{2(p+1)^2}$
4	$1 - \frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)}$
5	1

Results A: quadrics in n variables (2)

Theorem (A2)

The probability $\rho_n(p)$ that a random n-ary quadric over $\mathbb{Z}_p$ is isotropic over $\mathbb{Q}_p$ is

n	$\rho_n(p)$
1	0
2	$1/2$
3	$1 - \frac{p}{2(p+1)^2}$
4	$1 - \frac{p^3}{4(p+1)^2(p^4+p^3+p^2+p+1)}$
5	1

Our proof is uniform in p and n, and gives a new proof that all quadrics in ≥ 5 variables are isotropic over $\mathbb{Q}_p$, as well as an algorithm for deciding isotropy for $n \leq 4$.

Results A: quadrics in n variables (3)

Theorem (A3, joint also with J. Keating and N. Jones (Bristol))

The probability that a GOE-random n-ary quadric over $\mathbb{R}$ is isotropic is

$$\rho_n^{GOE}(\infty) = 1 - \frac{\mathrm{Pf}(S)}{2^{(n-1)(n+4)/4} \prod_{m=1}^{n} \Gamma(m/2)},$$

where S is the skew-symmetric matrix of size $2\lceil n/2 \rceil$ whose i,j entry is

$$\begin{cases} 2^{i+j-2}\Gamma\left(\frac{i+j}{2}\right)\left(\beta_{\frac{1}{2}}(\frac{i}{2},\frac{j}{2}) - \beta_{\frac{1}{2}}(\frac{j}{2},\frac{i}{2})\right) & \text{for } i < j \leq n \\ 2^{i-1}\Gamma\left(\frac{i}{2}\right) & \text{for } i < j = n+1 \text{ (n odd)} \end{cases}$$

Results A: quadrics in n variables (4)

Table of values of $\rho_n^{GOE}(\infty)$, the probability that a random real quadratic form is isotropic:

n	$\rho_n^{GOE}(\infty)$	
1	0	0
2	$\frac{1}{2}\sqrt{2}$	0.7071067811
3	$\frac{1}{2}+\sqrt{2}\pi^{-1}$	0.9501581580
4	$\frac{1}{2}+\frac{1}{8}\sqrt{2}+\pi^{-1}$	0.9950865814
5	$\frac{3}{4}+(\frac{2}{3}+\frac{1}{12}\sqrt{2})\pi^{-1}$	0.9997197706
6	$\frac{3}{4}+\frac{7}{64}\sqrt{2}+(\frac{37}{48}-\frac{1}{3}\sqrt{2})\pi^{-1}$	0.9999907596
7	$\frac{7}{8}+(\frac{47}{120}+\frac{109}{480}\sqrt{2})\pi^{-1}-\frac{32}{45}\sqrt{2}\pi^{-2}$	0.9999998239
$\ldots$	$\ldots$	$\ldots$
n	$\in \mathbb{Q}(\sqrt{2})[\pi^{-1}]$	≈ 1

Results A: quadrics in n variables (5)

Corollary

If D=U or GOE then

$$\rho_n^D(\mathbb{Q}) = \begin{cases} 0 & \text{if } n \leq 3; \\ \rho_4^D(\infty) \prod_p \left(1 - \frac{p^3(p-1)}{4(p+1)^2(p^5-1)}\right) & \text{if } n = 4; \\ \rho_n^D(\infty) & \text{if } n \geq 5. \end{cases}$$

In particular,

$$\rho_4^{GOE}(\mathbb{Q}) = \left(\frac{1}{2} + \frac{1}{8}\sqrt{2} + \frac{1}{\pi}\right) \prod_p \left(1 - \frac{p^3(p-1)}{4(p+1)^2(p^5-1)}\right)$$
$$\approx 0.983,$$

$\rho_n^{GOE}(\mathbb{Q}) = \rho_n^{GOE}(\infty) > 0.999$ *for* $n \geq 5$*, and* $\rho_n^{GOE}(\mathbb{Q}) = 0$ *for* $n \leq 3$.

Local questions B: ternary cubics

For plane cubics we can similarly define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^{10}$) ternary cubic form over $\mathbb{Z}_p$ has a $\mathbb{Q}_p$-rational point. We will give a uniform formula for this for all primes p.

Local questions B: ternary cubics

For plane cubics we can similarly define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^{10}$) ternary cubic form over $\mathbb{Z}_p$ has a $\mathbb{Q}_p$-rational point. We will give a uniform formula for this for all primes p.

Instead of global solubility, we define $\rho(\mathbb{Q})$ to be the probability that a random integral ternary cubic has $\mathbb{Q}_p$-rational points for all p.

Local results B: plane cubics

Since for cubics real solubility is automatic, we do not need to specify a distribution on the space $\mathbb{R}^{10}$.
As with quartics we find that the the probability of a random integral ternary cubic (with respect to any nice distribution) has a $\mathbb{Q}_p$-point is the same as $\rho(p)$, the probability that a random cubic over $\mathbb{Z}_p$ has a $\mathbb{Q}_p$-point.
The Poonen-Voloch result mentioned above implies

Theorem (B1)

$\rho(\mathbb{Q}) = \prod_p \rho(p)$.

(recall that here $\rho(\mathbb{Q})$ is the probability of everywhere local solubility, not of global solubility).

Local results B: plane cubics (continued)

Theorem (B2)

For all primes p, the probability that a random plane cubic over $\mathbb{Q}_p$ has a $\mathbb{Q}_p$-rational point is

$$\rho(p) = 1 - f(p)/g(p),$$

where

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

Note that $f(p)/g(p) \sim 1/3p^3$, so $\rho(p) \to 1$ rapidly as $p \to \infty$: $\rho(2) = 0.98319$, $\rho(3) = 0.99259$, $\rho(5) = 0.99799$, $\rho(7) = 0.99918$.

Local results B: plane cubics (concluded)

Corollary (B3)

A random integral plane cubic is everywhere locally soluble with probability $\rho(\mathbb{Q}) = \prod_p (1 - f(p)/g(p)) \approx 0.97256$.

Local results B: plane cubics (concluded)

Corollary (B3)

A random integral plane cubic is everywhere locally soluble with probability $\rho(\mathbb{Q}) = \prod_p (1 - f(p)/g(p)) \approx 0.97256$*.*

Remark

It is unexpected that $\rho(p)$ *be given by a single rational function of* p*. On general grounds it is expected, according to Denef and Loeser, to be expressable as a rational function of the counts of* $\mathbb{F}_p$*-points on a finite number of* $\mathbb{Z}$*-schemes. In our proof of Theorem B2, we treat all primes uniformly throughout.*

Local results B: plane cubics (concluded)

Corollary (B3)

A random integral plane cubic is everywhere locally soluble with probability $\rho(\mathbb{Q}) = \prod_p (1 - f(p)/g(p)) \approx 0.97256$.

Remark

It is unexpected that $\rho(p)$ be given by a single rational function of p. On general grounds it is expected, according to Denef and Loeser, to be expressable as a rational function of the counts of $\mathbb{F}_p$-points on a finite number of $\mathbb{Z}$-schemes. In our proof of Theorem B2, we treat all primes uniformly throughout.

Remark

Corollary B3 is used in Manjul Bhargava's result that a positive proportion of plane cubics fail the Hasse principle.

Local questions C: elliptic quartics

Here we define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^5$) binary quartic form $f(X, Y)$ over $\mathbb{Z}_p$ is soluble in the sense that the curve $Z^2 = f(X, Y)$ has a $\mathbb{Q}_p$-rational point. We give a formula for all *odd* primes p which needs adjustment at $p = 2$.

Local questions C: elliptic quartics

Here we define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^5$) binary quartic form $f(X,Y)$ over $\mathbb{Z}_p$ is soluble in the sense that the curve $Z^2 = f(X,Y)$ has a $\mathbb{Q}_p$-rational point. We give a formula for all *odd* primes p which needs adjustment at $p = 2$.

However, if we instead consider *generalized binary quartics*, equations of the form $Z^2 + g(X,Y)Z = f(X,Y)$ with $\deg(g) = 2$ and $\deg(f) = 4$, distributed over $\mathbb{Z}_p^8$, then we obtain a uniform formula for all p (which agrees with the non-generalized formula for odd p).

Local questions C: elliptic quartics

Here we define $\rho(p)$ to be the probability that a random (with respect to the p-adic measure on $\mathbb{Z}_p^5$) binary quartic form $f(X, Y)$ over $\mathbb{Z}_p$ is soluble in the sense that the curve $Z^2 = f(X, Y)$ has a $\mathbb{Q}_p$-rational point. We give a formula for all *odd* primes p which needs adjustment at $p = 2$.

However, if we instead consider *generalized binary quartics*, equations of the form $Z^2 + g(X, Y)Z = f(X, Y)$ with $\deg(g) = 2$ and $\deg(f) = 4$, distributed over $\mathbb{Z}_p^8$, then we obtain a uniform formula for all p (which agrees with the non-generalized formula for odd p).

Again, instead of global solubility, we define $\rho(\mathbb{Q})$ to be the probability that a random integral binary quartic quartic has $\mathbb{Q}_p$-rational points for all p and real points; here we need to specify a distribution D on $\mathbb{R}^5$.

Local results C: binary quartics (1)

Theorem (C1)

The density $\rho(p)$ of binary quartic forms $f(X,Y) \in \mathbb{Z}_p[X,Y]$ for which the curve $Z^2 = f(X,Y)$ has a $\mathbb{Q}_p$-rational point is

$$\rho(p) = \frac{F(p)}{G(p)} = \frac{8p^{10} + 8p^9 - 4p^8 + 2p^6 + p^5 - 2p^4 + p^3 - p^2 - 8p - 5}{8(p+1)(p^9 - 1)}$$

for $p \geq 3$, and

$$\rho(2) = \frac{23087}{24529}.$$

The density in $\mathbb{Z}_p^8$ of pairs of forms $f, g \in \mathbb{Z}_p[X,Y]$ of degree 4 and 2 for which the curve $Z^2 + g(X,Y)Z = f(X,Y)$ has a $\mathbb{Q}_p$-rational point is $\rho(p)$ (as above) for $p \geq 3$ and for $p = 2$ is $\rho'(2) = F(2)/G(2) = 11887/12264$.

Local results C: binary quartics (2)

Our proof of Theorem C1 works only with the case of generalized binary quartics, and is completely uniform in p. At the end we deduce the "non-generalized" version by computing the proportion of generalized equations which can be put into the simple form (which is 1 for odd p).

Local results C: binary quartics (2)

Our proof of Theorem C1 works only with the case of generalized binary quartics, and is completely uniform in p. At the end we deduce the “non-generalized” version by computing the proportion of generalized equations which can be put into the simple form (which is 1 for odd p).

Over $\mathbb{R}$ we have not yet been able to derive an exact formula for $\rho^D(\mathbb{R})$, the probability that a random real quartic f is not negative definite (so that $Z^2 = f(X,Y)$ has real solutions), for some distribution D on the space of all real binary quartics. A numerical approximation to this (for the uniform distribution) is between 0.872 and 0.875. However, it may be that (as for random real symmetric matrices) there is a better distribution to use than the uniform one, for which an exact expression can be obtained. Work in progress!

Global results C: binary quartics

Theorem (C2)

When genus 1 *curves of the form* $Z^2 = f(X,Y)$, *with* $f \in \mathbb{Z}[X,Y]$ *homogeneous quartic, are ordered by the height of* f, *the proportion which are everywhere locally soluble is*

$$\rho(\mathbb{Q}) = \rho(\mathbb{R}) \cdot \frac{23087}{24529} \cdot \prod_{p \geq 3} \frac{F(p)}{G(p)} \approx 0.759.$$

Remarks on higher genus hyperelliptic curves

We only have partial results so far for higher genus curves, given by equations $Z^2 = f(X,Y)$ where f is homogeneous of degree $2g+2$:

Remarks on higher genus hyperelliptic curves

We only have partial results so far for higher genus curves, given by equations $Z^2 = f(X,Y)$ where f is homogeneous of degree $2g+2$:

- the local density $\rho_g(p)$ is a rational function of p for all $p \gg 0$.
- we have upper and lower bounds for ρ_g which are quite close, and hope to deduce some limiting results as $g \to \infty$.
- an exact formula for $\rho_2(p)$ is within reach; for small primes separate treatment is needed, since a smooth curve of genus $g > 1$ over $\mathbb{F}_p$ need not have any $\mathbb{F}_p$-rational points! This does not happen when $g = 1$.

Sketch of proof method (plane cubics) (1)

Let $C \in \mathbb{Z}_p[X,Y,Z]$ be a cubic form; its reduction $\overline{C} \in \mathbb{F}_p[X,Y,Z]$ is one of $p^{10}-1$ possible forms over $\mathbb{F}_p$ (or 0), and we divide into cases, each of which must be counted precisely to give the probability of being in that case.

Sketch of proof method (plane cubics) (1)

Let $C \in \mathbb{Z}_p[X,Y,Z]$ be a cubic form; its reduction $\overline{C} \in \mathbb{F}_p[X,Y,Z]$ is one of $p^{10}-1$ possible forms over $\mathbb{F}_p$ (or 0), and we divide into cases, each of which must be counted precisely to give the probability of being in that case.

- if $\overline{C}(\mathbb{F}_p)$ has a smooth point, it lifts and $C(\mathbb{Q}_p) \neq \emptyset$;
- if $\overline{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$;
- otherwise $\overline{C}(\mathbb{F}_p)$ consists of one or more singular points, and we "blow up" these in a recursive fashion.

Sketch of proof method (plane cubics) (1)

Let $C \in \mathbb{Z}_p[X, Y, Z]$ be a cubic form; its reduction $\overline{C} \in \mathbb{F}_p[X, Y, Z]$ is one of $p^{10} - 1$ possible forms over $\mathbb{F}_p$ (or 0), and we divide into cases, each of which must be counted precisely to give the probability of being in that case.

- if $\overline{C}(\mathbb{F}_p)$ has a smooth point, it lifts and $C(\mathbb{Q}_p) \neq \emptyset$;
- if $\overline{C}(\mathbb{F}_p) = \emptyset$, then $C(\mathbb{Q}_p) = \emptyset$;
- otherwise $\overline{C}(\mathbb{F}_p)$ consists of one or more singular points, and we "blow up" these in a recursive fashion.

The only configuration for which we can conclude that $C(\mathbb{Q}_p) = \emptyset$ is when $\overline{C}$ is a product of 3 non-concurrent lines, defined and conjugate over $\mathbb{F}_{p^3}$.

Sketch of proof method (plane cubics) (2)

The two configurations for which we must recurse are when $\overline{C}$ is a product of 3 concurrent lines, defined and conjugate over $\mathbb{F}_{p^3}$, when the only $\mathbb{F}_p$-point is the intersection, which is singular; or a triple line $C = L^3$ on which all $\mathbb{F}_p$-points are singular.

Sketch of proof method (plane cubics) (2)

The two configurations for which we must recurse are when $\overline{C}$ is a product of 3 concurrent lines, defined and conjugate over $\mathbb{F}_{p^3}$, when the only $\mathbb{F}_p$-point is the intersection, which is singular; or a triple line $C = L^3$ on which all $\mathbb{F}_p$-points are singular.

For example, if $\overline{C} = L^3$, with loss $C \equiv X^3$, so any primitive point has $X \equiv 0 \pmod{p}$, so we replace X by pX, divide by p and continue, dividing into cases as before (but the counts are not the same).

Sketch of proof method (plane cubics) (2)

The two configurations for which we must recurse are when $\overline{C}$ is a product of 3 concurrent lines, defined and conjugate over $\mathbb{F}_{p^3}$, when the only $\mathbb{F}_p$-point is the intersection, which is singular; or a triple line $C = L^3$ on which all $\mathbb{F}_p$-points are singular.

For example, if $\overline{C} = L^3$, with loss $C \equiv X^3$, so any primitive point has $X \equiv 0 \pmod{p}$, so we replace X by pX, divide by p and continue, dividing into cases as before (but the counts are not the same).

After a finite number of steps we always return to a configuration seen before. This leads to a system of linear equations for the probabilities, which have a unique solution.

All the counts and conditional probabilities are rational functions of p (and all this generalises to unramified extensions of $\mathbb{Q}_p$, simply replacing p by q in all formulae), and nowhere is the specific value of p relevant.