On a dense universal Hilbert set

Michael Filaseta

University of South Carolina

joint work with Robert Wilcox

An explicit dense universal Hilbert set, Math. Proc. Camb. Phil. Soc. 167 (2019), 531–547.

Theorem (Hilbert, 1892). *For each positive integer n, there is a polynomial in $\mathbb{Q}[x]$ with associated Galois group S_n, the symmetric group on n letters. For each positive integer n, there is also a polynomial in $\mathbb{Q}[x]$ with associated Galois group A_n, the alternating group on n letters.*

Idea: Find an irreducible polynomial $F(x,y) \in \mathbb{Q}[x,y]$ for which the Galois group of $F(x,y)$ over $Q(y)$ is S_n (or A_n). Pick $y = y^* \in \mathbb{Q}$ so that $F(x,y^*)$ is irreducible over $\mathbb{Q}$. Then $f(x) = F(x,y^*)$ will have Galois group S_n (or A_n) over $\mathbb{Q}$.

Theorem (Ibidem). *If $F(x,y)$ is irreducible in $\mathbb{Q}[x,y]$, then there are infinitely many $y^* \in \mathbb{Q}$ such that $f(x) = F(x,y^*)$ is irreducible in $\mathbb{Q}[x]$.*

Hilbert's Irreducibility Theorem. *Let*

$$f_1(x_1,\dots,x_r,y_1,\dots,y_s),\dots,f_m(x_1,\dots,x_r,y_1,\dots,y_s)$$

be irreducible polynomials in $\mathbb{Q}[x_1,\dots,x_r,y_1,\dots,y_s]$. Then there exists infinitely choices of rational numbers $y_1^*,\dots,y_s^*$ for which

$$f_1(x_1,\dots,x_r,y_1^*,\dots,y_s^*),\dots,f_m(x_1,\dots,x_r,y_1^*,\dots,y_s^*)$$

are irreducible in $\mathbb{Q}[x_1,\dots,x_r]$.

Comments and Improvements:

- Hilbert's original proof was ineffective (not providing a method for finding $y_1^*,\dots,y_s^*$).
- One can find such $y_1^*,\dots,y_s^*$ in $\mathbb{Z}$.
- The "good" $(y_1^*,\dots,y_s^*) \in \mathbb{Z}^s$ have density 1 in $\mathbb{Z}^s$.
- There are arithmetic progressions $P_1,\dots,P_s$ such that if each $y_j^* \in P_j$, then $(y_1^*,\dots,y_s^*)$ is good.

Hilbert's Irreducibility Theorem. *Let*

$$f_1(x_1,\dots,x_r,y_1,\dots,y_s),\dots,f_m(x_1,\dots,x_r,y_1,\dots,y_s)$$

be irreducible polynomials in $\mathbb{Q}[x_1,\dots,x_r,y_1,\dots,y_s]$. Then there exists infinitely choices of rational numbers $y_1^*,\dots,y_s^*$ for which

$$f_1(x_1,\dots,x_r,y_1^*,\dots,y_s^*),\dots,f_m(x_1,\dots,x_r,y_1^*,\dots,y_s^*)$$

are irreducible in $\mathbb{Q}[x_1,\dots,x_r]$.

A. Schinzel and U. Zannier, 1995

- If $r = s = 1$ (and m arbitrary), an explicit upper bound can be given for positive integers y_1^* in $\mathbb{Z}$ as above. With

$$d_x = \max_{1\le j\le m}\{\deg_x f_j\}, \quad d_y = \max_{1\le j\le m}\{\deg_y f_j\} \quad \text{and}$$

$$H = \max\{20, H(f_1),\dots,H(f_m)\} \quad (H(f) = \text{height of } f),$$

$$y_1^* \le \max\{\exp(36^6), \exp(2(6d_y)^5), m^9 \exp(450(\log H)^{5/6} + 11250d_y^5 + 45(d_y+1)^2 d_x + 45d_x(\log H)^{2/5})\}.$$

Hilbert's Irreducibility Theorem. *Let*

$$f_1(x_1,\dots,x_r,y_1,\dots,y_s),\dots,f_m(x_1,\dots,x_r,y_1,\dots,y_s)$$

be irreducible polynomials in $\mathbb{Q}[x_1,\dots,x_r,y_1,\dots,y_s]$. Then there exists infinitely choices of rational numbers $y_1^*,\dots,y_s^*$ for which

$$f_1(x_1,\dots,x_r,y_1^*,\dots,y_s^*),\dots,f_m(x_1,\dots,x_r,y_1^*,\dots,y_s^*)$$

are irreducible in $\mathbb{Q}[x_1,\dots,x_r]$.

- Wiles used Hilbert's Irreducibility Theorem in his proof of Fermat's Last Theorem; it is now known that one can replace its use with an application of Faltings' theorem.

Hilbert's Irreducibility Theorem (roughly): An irreducible polynomial in several variables can find infinitely many specializations of some preselected variables so that the resulting polynomial remains irreducible in the remaining variables.

$F(x,y) \in \mathbb{Z}[x,y]$, irreducible in $\mathbb{Q}[x,y]$ and $\deg_x(F) \ge 1$

Example. Let $f(x)$ and $g(x)$ be relatively prime polynomials in $\mathbb{Z}[x]$ with $f(x)\,g(x)$ non-constant. Then taking $F(x,y) = f(x) + y\,g(x)$, we deduce there are infinitely many integers k such that

$$f(x) + k\,g(x)$$

is irreducible over $\mathbb{Q}$.

Hilbert's Irreducibility Theorem (roughly): An irreducible polynomial in several variables can find infinitely many specializations of some preselected variables so that the resulting polynomial remains irreducible in the remaining variables.

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Example. Let $f(x) \in \mathbb{Z}[x]$, and suppose that for $n \in \mathbb{Z}$ with $|n|$ sufficiently large, we have $f(n)$ is a square. Then $f(x) = g(x)^2$ for some $g(x) \in \mathbb{Z}[x]$.

Proof. Let $F(x, y) = x^2 - f(y)$. Hilbert's Irreducibility Theorem implies $F(x, y)$ is reducible. This implies $f(y)$ is a square in $\mathbb{Z}[y]$. ■

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Known: For almost all $y_0 \in \mathbb{Z}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

$|\{y_0 \in \mathbb{Z} : |y_0| \leq Y, F(x, y_0) \text{ is reducible in } \mathbb{Q}[x]\}| = o(Y)$

Comment: More can be said based on Siegel's Lemma. (In fact, this work was motivated by a desire to find a simple explanation for the above asymptotic based on Siegel's Lemma.)

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Known: For almost all $y_0 \in \mathbb{Z}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x, y) \in \mathbb{Z}[x, y]$ which is irreducible in $\mathbb{Q}[x, y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

- There are finitely many $y_0 \in \mathcal{S}$ with $F(x, y_0)$ reducible.
- The set $\mathcal{S}$ is fixed - independent of $F(x, y) \in \mathbb{Z}[x, y]$.

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x, y) \in \mathbb{Z}[x, y]$ which is irreducible in $\mathbb{Q}[x, y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

- There are finitely many $y_0 \in \mathcal{S}$ with $F(x, y_0)$ reducible.
- The set $\mathcal{S}$ is fixed - independent of $F(x, y) \in \mathbb{Z}[x, y]$.

Comment: The example $F(x, y) = x^2 - y$ shows that $\mathbb{Z}$ is not a universal Hilbert set. In fact, it shows that any universal Hilbert set can contain at most finitely many squares (and, similarly, k^{th} powers).

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x, y) \in \mathbb{Z}[x, y]$ which is irreducible in $\mathbb{Q}[x, y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

The existence of universal Hilbert sets was first shown in

P. C. Gilmore and A. Robinson, *Metamathematical considerations on the relative irreducibility of polynomials*, Canad. J. Math., 7 (1955), 483–489.

$F(x, y) \in \mathbb{Z}[x, y]$, irreducible in $\mathbb{Q}[x, y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x, y) \in \mathbb{Z}[x, y]$ which is irreducible in $\mathbb{Q}[x, y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x, y_0)$ is irreducible in $\mathbb{Q}[x]$.

First example given was

$$\mathcal{S} = \left\{ \left\lfloor \exp\left(\sqrt{\log\log n}\right) \right\rfloor + n!\, 2^{n^2} : n \in \mathbb{Z}, n \geq 3 \right\}.$$

V. G. Sprindžuk, *Diophantine equations involving unknown prime numbers*, Trudy Math. Inst. Steklov 158 (1981), 180–196; English transl. in Proc. Steklov Inst. Math. 1983, Issue 4, 197–214.

$F(x,y) \in \mathbb{Z}[x,y]$, irreducible in $\mathbb{Q}[x,y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x,y) \in \mathbb{Z}[x,y]$ which is irreducible in $\mathbb{Q}[x,y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x,y_0)$ is irreducible in $\mathbb{Q}[x]$.

$$\mathcal{S} = \{\lfloor \exp(\sqrt{\log\log n})\rfloor + n!\, 2^{n^2} : n \in \mathbb{Z}, n \geq 3\}.$$

Other Examples of $\mathcal{S}$:

$\{2^n + 3^n : n \in \mathbb{N}\}$ (Corvaja and Zannier, 1998)

$\{2^n + n : n \in \mathbb{N}\}$ (Dèbes and Zannier, 1998)

$\{\lfloor \log\log|n|\rfloor + n^3 : n \in \mathbb{Z}, |n| \geq 3\}$ (Bilu, 1996)

$\{p_n \prod_{p_i \leq \log\log n} p_i : n \in \mathbb{Z}, n \geq 3\}$ (Zannier, 1996)

$F(x,y) \in \mathbb{Z}[x,y]$, irreducible in $\mathbb{Q}[x,y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x,y) \in \mathbb{Z}[x,y]$ which is irreducible in $\mathbb{Q}[x,y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x,y_0)$ is irreducible in $\mathbb{Q}[x]$.

$\{2^n + 3^n : n \in \mathbb{N}\}$ (Corvaja and Zannier, 1998)

$\{2^n + n : n \in \mathbb{N}\}$ (Dèbes and Zannier, 1998)

$\{\lfloor \log\log|n|\rfloor + n^3 : n \in \mathbb{Z}, |n| \geq 3\}$ (Bilu, 1996)

$\{p_n \prod_{p_i \leq \log\log n} p_i : n \in \mathbb{Z}, n \geq 3\}$ (Zannier, 1996)

Comment: The papers by Bilu and by Dèbes and Zannier further show that there exist universal Hilbert sets with asymptotic density 1 in the integers (without giving an explicit example of such a set).

$F(x,y) \in \mathbb{Z}[x,y]$, irreducible in $\mathbb{Q}[x,y]$ and $\deg_x(F) \geq 1$

Definition: A *universal Hilbert set* is an infinite set $\mathcal{S} \subseteq \mathbb{Z}$ having the property that for every $F(x,y) \in \mathbb{Z}[x,y]$ which is irreducible in $\mathbb{Q}[x,y]$ and satisfies $\deg_x(F) \geq 1$, we have that for all but finitely many $y_0 \in \mathcal{S}$, the polynomial $F(x,y_0)$ is irreducible in $\mathbb{Q}[x]$.

Comment: The papers by Bilu and by Dèbes and Zannier further show that there exist universal Hilbert sets with asymptotic density 1 in the integers (without giving an explicit example of such a set).

Main Result (with R. Wilcox): There exists an explicit universal Hilbert set $\mathcal{S} \subset \mathbb{Z}$ for which

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \leq X\}| \ll \frac{X}{(\log X)^\delta}$$

as $X \to \infty$, where

$$\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots.$$

Example. Let $f(x,y) = x^4 + (y+8)x - y^2 - y$. Then $f(x,y_0)$ is irreducible in $\mathbb{Z}[x]$ for $y_0 \in \mathbb{Z}$ if and only if $y_0 \notin \{-96, -39, -3, -1, 0, 3, 7, 32, 105\}$.

Let $g(x) \in \mathbb{Z}[x]$ be an irreducible factor of $f(x,y_0)$ of smallest positive degree. We are interested in knowing for what $y_0 \in \mathbb{Z}$, we have $\deg g \in \{1, 2\}$.

Case 1. $g(x) = x - a$

Case 2. $g(x) = x^2 + ax + b$

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 1. $g(x) = x - a$

$$y^2 + (1-a)y - a^4 - 8a = 0$$

$$(1-a)^2 + 4a^4 + 32a = 4a^4 + a^2 + 30a + 1$$

$$w^2 = 4a^4 + a^2 + 30a + 1$$

Comment. The above is an equation for an elliptic curve and will have finitely many integer points on it. Software packages can be used to find the integer points, but some caution is needed. For example, Sage currently provides a method for one to find the integer points on an elliptic curve given in Weierstrass form, so we can express the elliptic curve in Weierstrass form. But integer points on the curve above may now correspond to rational points on the elliptic curve in Weierstrass form.

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 1. $g(x) = x - a$

$$y^2 + (1-a)y - a^4 - 8a = 0$$

$$(1-a)^2 + 4a^4 + 32a = 4a^4 + a^2 + 30a + 1$$

$$(4w)^2 = 64a^4 + 16a^2 + 480a + 16 = (8a^2+1)^2 + 480a + 15$$

$$a \in \mathbb{Z} \implies 480a + 15 \neq 0$$

If $480a + 15 > 0$, then

$$64a^4 + 16a^2 + 480a + 16 = (4w)^2 \geq 64a^4 + 64a^2 + 16,$$

so $0 \leq a \leq 10$.

If $480a + 15 < 0$, then

$$64a^4 + 16a^2 + 480a + 16 = (4w)^2 \leq (8a^2 - 4)^2 = 64a^4 - 64a^2 + 16,$$

so $-6 \leq a < 0$.

$$\boxed{-6 \leq a \leq 10}$$

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 1. $g(x) = x - a$

$$y^2 + (1-a)y - a^4 - 8a = 0$$

$$(1-a)^2 + 4a^4 + 32a = 4a^4 + a^2 + 30a + 1$$

$$(4w)^2 = 64a^4 + 16a^2 + 480a + 16 = (8a^2+1)^2 + 480a + 15$$

$$a \in \mathbb{Z} \implies 480a + 15 \neq 0$$

$$\boxed{-6 \leq a \leq 10}$$

$$y \in \{-96, -39, -3, -1, 0, 3, 32, 105\}$$

For $y = 105$, the quartic $x^4 + (y+8)\,x - y^2 - y$ becomes

$$x^4 + (105+8)\,x - 105^2 - 105 = x^4 + 113\,x - 11130$$
$$= (x-10)\,(x^3 + 10\,x^2 + 100\,x + 1113).$$

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 2. $g(x) = x^2 + ax + b$

"$f(x)$" divided by $g(x)$ gives a remainder of

$$(-a^3 + 2\,ab + y + 8)\,x - a^2b + b^2 - y^2 - y$$

$$-a^3 + 2\,ab + y + 8 = 0 \quad \text{and} \quad -a^2b + b^2 - y^2 - y = 0$$

Viewing a and y as fixed,
the two equations have a common root in b.

$$\mathrm{Res}(-a^3 + 2\,ab + y + 8, -a^2b + b^2 - y^2 - y, b) = 0$$

UNIVERSITY OF SOUTH CAROLINA

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 2. $g(x) = x^2 + ax + b$

$$(-a^3 + 2\,ab + y + 8)\,x - a^2b + b^2 - y^2 - y$$

$$-a^3 + 2\,ab + y + 8 = 0 \quad \text{and} \quad -a^2b + b^2 - y^2 - y = 0$$

$$\mathrm{Res}(-a^3 + 2\,ab + y + 8, -a^2b + b^2 - y^2 - y, b) = 0$$

$$-a^6 - 4\,a^2y^2 - 4\,a^2y + y^2 + 16\,y + 64 = 0$$

Siegel's Theorem

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 2. $g(x) = x^2 + ax + b$

$$-a^3 + 2\,ab + y + 8 = 0 \quad \text{and} \quad -a^2b + b^2 - y^2 - y = 0$$

$$\mathrm{Res}(-a^3 + 2\,ab + y + 8, -a^2b + b^2 - y^2 - y, b) = 0$$

$$-a^6 - 4\,a^2y^2 - 4\,a^2y + y^2 + 16\,y + 64 = 0$$

$$w^2 = -16\,a^8 + 4\,a^6 + 16\,a^4 + 896\,a^2$$
$$= -4\,(a-2)\,(a+2)\,(4\,a^4 + 15\,a^2 + 56)\,a^2$$

$$a \in \{-2, -1, 0, 1, 2\}$$

$$y \in \{-3, 0, 7\}$$

$$y = 7 \longmapsto x^4 + 15x - 56 = (x^2 + x - 7)\,(x^2 - x + 8)$$

$$\boxed{f(x,y) = x^4 + (y+8)x - y^2 - y}$$

Case 1. $g(x) = x - a$

$$y \in \{-96, -39, -3, -1, 0, 3, 32, 105\}$$

Case 2. $g(x) = x^2 + ax + b$

$$y \in \{-3, 0, 7\}$$

Example. Let $f(x,y) = x^4 + (y+8)x - y^2 - y$. Then $f(x, y_0)$ is irreducible in $\mathbb{Z}[x]$ for $y_0 \in \mathbb{Z}$ if and only if $y_0 \notin \{-96, -39, -3, -1, 0, 3, 7, 32, 105\}$.

Main Result (with R. Wilcox): There exists an explicit universal Hilbert set $\mathcal{S} \subset \mathbb{Z}$ for which

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \leq X\}| \ll \frac{X}{(\log X)^\delta}$$

as $X \to \infty$, where

$$\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots.$$

Comments: There are 461845 elements of $\mathcal{S}$ up to 10^6. Although the expression $X/(\log X)^\delta$ on the right of is $o(X)$ as $X \to \infty$, it is $> X/2$ for $1 < X \leq 10^{1365}$.

What's $\mathcal{S}$? (Warning: It is not aesthetically pleasing.)

Where is δ coming from?

Main Result (with R. Wilcox): There exists an explicit universal Hilbert set $\mathcal{S} \subset \mathbb{Z}$ for which

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \le X\}| \ll \frac{X}{(\log X)^{\delta}}$$

as $X \to \infty$, where

$$\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots.$$

What's $\mathcal{S}$? (Warning: It is not aesthetically pleasing.)

For integers $j \ge 3$, $k \ge 2$, ℓ and ℓ' with $\ell \ne 0$, set

$$Y(j,k,\ell,\ell') = \Big\{ m \in \mathbb{Z} : \ |m| \in (2^j, 2^{j+1}] \text{ and } |\ell m + \ell'| \text{ has no divisor in } \Big(\frac{2^{j/k}}{\log\log j}, 2^{j/k}\log\log j\Big]\Big\}.$$

What's $\mathcal{S}$? (Warning: It is not aesthetically pleasing.)

For integers $j \ge 3$, $k \ge 2$, ℓ and ℓ' with $\ell \ne 0$, set

$$Y(j,k,\ell,\ell') = \Big\{ m \in \mathbb{Z} : \ |m| \in (2^j, 2^{j+1}] \text{ and } |\ell m + \ell'| \text{ has no divisor in } \Big(\frac{2^{j/k}}{\log\log j}, 2^{j/k}\log\log j\Big]\Big\}.$$

For $j \ge 3$, let

$$M(j) = \max\{2, \log\log\log j\}.$$

Then

$$\mathcal{S} = \bigcup_{j=3}^{\infty} \bigcap_{2\le k\le M(j)} \bigcap_{\substack{-M(j)\le \ell\le M(j)\\ \ell\ne 0}} \bigcap_{-M(j)\le \ell'\le M(j)} Y(j,k,\ell,\ell').$$

$$Y(j,k,\ell,\ell') = \Big\{ m \in \mathbb{Z} : \ |m| \in (2^j, 2^{j+1}] \text{ and } |\ell m + \ell'| \text{ has no divisor in } \Big(\frac{2^{j/k}}{\log\log j}, 2^{j/k}\log\log j\Big]\Big\}$$

$$M(j) = \max\{2, \log\log\log j\}$$

$$\mathcal{S} = \bigcup_{j=3}^{\infty} \bigcap_{2\le k\le M(j)} \bigcap_{\substack{-M(j)\le \ell\le M(j)\\ \ell\ne 0}} \bigcap_{-M(j)\le \ell'\le M(j)} Y(j,k,\ell,\ell')$$

Main Result (with R. Wilcox): There exists an explicit universal Hilbert set $\mathcal{S} \subset \mathbb{Z}$ for which

$$|\{m \in \mathbb{Z} : m \notin \mathcal{S}, |m| \le X\}| \ll \frac{X}{(\log X)^{\delta}}$$

as $X \to \infty$, where

$$\delta = 1 - (1 + \log\log 2)/(\log 2) = 0.086071\ldots.$$

Where is δ coming from?

Theorem (Ford, 2008). *Let x, y and z be real numbers with $x \ge 10^5$, $100 \le y \le \sqrt{x}$, $2y \le z \le y^2$ and $z \le x$. Set $H(x,y,z)$ to be the number of positive integers $n \le x$ for which some divisor d of n satisfies $d \in (y,z]$. Set*

$$u = \frac{\log z}{\log y} - 1,$$

and let $\delta = 1-(1+\log\log 2)/(\log 2) = 0.086071\ldots$. Then

$$\frac{H(x,y,z)}{x} \asymp u^{\delta}\big(\log(2/u)\big)^{-3/2}.$$

Where is δ coming from?

Theorem (Ford, 2008). *Let x, y and z be real numbers with $x \ge 10^5$, $100 \le y \le \sqrt{x}$, $2y \le z \le y^2$ and $z \le x$. Set $H(x,y,z)$ to be the number of positive integers $n \le x$ for which some divisor d of n satisfies $d \in (y,z]$. Set*

$$u = \frac{\log z}{\log y} - 1,$$

and let $\delta = 1-(1+\log\log 2)/(\log 2) = 0.086071\ldots$. Then

$$\frac{H(x,y,z)}{x} \asymp u^{\delta}\big(\log(2/u)\big)^{-3/2}.$$

Another important ingredient we use is Siegel's Lemma.

Siegel's Lemma (Siegel, 1929). *Let $f(x,y)$ be in $\mathbb{Z}[x,y]$ with $f(x,y)$ irreducible in $\mathbb{C}[x,y]$. If there are infinitely many points $(x_0,y_0) \in \mathbb{Z}^2$ such that $f(x_0,y_0) = 0$, then there exist polynomials $u_j(t)$ and $v_j(t)$ in $\mathbb{Z}[t]$ for $j \in \{1,2\}$ satisfying both of the following:*

(i) For all but finitely many $(x',y') \in \mathbb{C}^2$ with $f(x',y') = 0$, the equations $x' = u_1(t)/v_1(t)$ and $y' = u_2(t)/v_2(t)$ hold for some $t \in \mathbb{C}$.

(ii) For all but finitely many $(x',y') \in \mathbb{Q}^2$ and $t \in \mathbb{C}$ such that $x' = u_1(t)/v_1(t)$ and $y' = u_2(t)/v_2(t)$, we have $t \in \mathbb{Q}$.

$F(x,y) \in \mathbb{Z}[x,y]$ irreducible in $\mathbb{Q}[x,y]$, $\deg F_x = n \geq 2$

Idea: For $k \in [1, n/2] \cap \mathbb{Z}$, show there are only finitely many $y_0 \in \mathcal{S}$ for which the polynomial $F(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$. We assume $F(x,y)$ is monic as a polynomial in x here. Suppose $y_0 \in \mathbb{Z}$ such that $F(x, y_0)$ is divisible by

$$H(x) = x^k + h_{k-1}x^{k-1} + \cdots + h_2x^2 + h_1x + h_0,$$

for some $h_j \in \mathbb{Z}$. Divide $F(x,y)$ by $H(x)$ as a polynomial in x to obtain a remainder

$$R(x) = r_{k-1}x^{k-1} + r_{k-2}x^{k-2} + \cdots + r_1x + r_0.$$

$r_j = r_j(h_0, \ldots, h_{k-1}, y) \in \mathbb{Z}[h_0, \ldots, h_{k-1}, y]$, $0 \leq j \leq k-1$

We deduce that for $y_0 \in \mathbb{Z}$, the following are equivalent:

- $F(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$.
- $\exists$ k-tuple $(h_0^*, \ldots, h_{k-1}^*) \in \mathbb{Z}^k$ with $r_j(h_0^*, \ldots, h_{k-1}^*, y_0) = 0$ for every $j \in \{0, 1, \ldots, k-1\}$.

$F(x,y) \in \mathbb{Z}[x,y]$ irreducible in $\mathbb{Q}[x,y]$, $\deg F_x = n \geq 2$

$$H(x) = x^k + h_{k-1}x^{k-1} + \cdots + h_2x^2 + h_1x + h_0,$$

for some $h_j \in \mathbb{Z}$. Divide $F(x,y)$ by $H(x)$ as a polynomial in x to obtain a remainder

$$R(x) = r_{k-1}x^{k-1} + r_{k-2}x^{k-2} + \cdots + r_1x + r_0.$$

$r_j = r_j(h_0, \ldots, h_{k-1}, y) \in \mathbb{Z}[h_0, \ldots, h_{k-1}, y]$, $0 \leq j \leq k-1$

We deduce that for $y_0 \in \mathbb{Z}$, the following are equivalent:

- $F(x, y_0)$ has a factor of degree k in $\mathbb{Z}[x]$.
- $\exists$ k-tuple $(h_0^*, \ldots, h_{k-1}^*) \in \mathbb{Z}^k$ with $r_j(h_0^*, \ldots, h_{k-1}^*, y_0) = 0$ for every $j \in \{0, 1, \ldots, k-1\}$.

We want the latter holds for only finitely many $y_0 \in \mathcal{S}$. To do this, we show that the variety

$$V(r_0, r_1, \ldots, r_{k-1})$$

over $\mathbb{C}$ intersected with $\mathbb{Z}^{k+1}$ has finitely many elements with y component in $\mathcal{S}$.

Idea: If this were a linear system of k equations in $k+1$ unknowns, then typically we would expect to be able to solve for each variable h_j in say y. For non-linear systems, using resultants, one can instead reduce our problem, for each j, to a polynomial in h_j and y equal to 0. This is a curve then in h_j and y and we can hope to apply Siegel's Lemma. The main problem is to show that when Siegel's Lemma does not apply directly, with some other ideas, one can still get what one wants.

The Genus 0 Case

Lemma 1. *Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with*

$$\gcd(f, g) = 1 \quad \textit{and} \quad \max\{\deg f, \deg g\} \geq 2.$$

Let $\mathcal{S}$ be the same mess as before. Let $\mathcal{Y}$ be the set of $y \in \mathbb{Z}$ for which $f(x) + yg(x)$ has a linear factor in $\mathbb{Z}[x]$. Then $\mathcal{Y} \cap \mathcal{S}$ is finite. Furthermore, if $\deg f > \deg g \geq 1$, then $\mathcal{Y}$ is finite.

Lemma 2. *Let $f(x,y)$ be in $\mathbb{Z}[x,y]$ with $f(x,y)$ irreducible in $\mathbb{C}[x,y]$. Let $\mathcal{S}$ be the same mess as before. Let $\mathcal{Y}'$ be the set of $y_0 \in \mathbb{Z}$ such that $f(x_0, y_0) = 0$ for some $x_0 \in \mathbb{Z}$. Then there is a rational function $\hat{h}(y) \in \mathbb{Q}(y)$ such that for all but finitely many $y_0 \in \mathcal{Y}' \cap \mathcal{S}$, the only integer x_0 satisfying $f(x_0, y_0) = 0$ is $x_0 = \hat{h}(y_0)$. Furthermore, in the case that $\mathcal{Y}' \cap \mathcal{S}$ is an infinite set, for all but finitely many $y_0 \in \mathbb{C}$, if $f(x_0, y_0) = 0$ for some $x_0 \in \mathbb{C}$, then $x_0 = \hat{h}(y_0)$.*

Theorem (R. Wilcox, F.) *Let $\mathcal{S}$ be as before. Let the variety*

$$V = V(r_0, r_1, \ldots, r_{k-1}),$$

with

$$r_j = r_j(h_0, \ldots, h_{k-1}, y) \in \mathbb{Z}[h_0, \ldots, h_{k-1}, y],$$

over the complex numbers have the property that for each $y_0 \in \mathbb{C}$, there are finitely many points $(h_0^*, \ldots, h_{k-1}^*) \in \mathbb{C}^k$ such that $(h_0^*, \ldots, h_{k-1}^*, y_0) \in V$. Suppose that there are infinitely many points $(h_0^*, \ldots, h_{k-1}^*, y_0)$ in $V \cap \mathbb{Z}^{k+1}$ with $y_0 \in \mathcal{S}$. Then there exist $\hat{h}_t(y) \in \mathbb{Q}(y)$ for $t \in \{0, 1, \ldots, k-1\}$ such that the set of

$$(\hat{h}_0(y_0), \ldots, \hat{h}_{k-1}(y_0), y_0) \in V \cap (\mathbb{Z}^k \times \mathcal{S})$$

is an infinite set.

The End