SQUAREFREE VALUES OF QUADRATIC POLYNOMIALS COURSE NOTES, 2015

ZEÉV RUDNICK

1. Squarefree values of polynomials: History

In this section we study the problem of representing square-free integers by integer polynomials. It is conjectured that a separable polynomial (that is, without repeated roots) $f \in \mathbb{Z}[x]$ takes infinitely many square-free values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is square-free have a positive density. A clear necessary condition is that the sequence $f(n)$ has no fixed square divisor; the conjecture is that this is the only obstruction:

Conjecture 1. *Let $f(x) \in \mathbb{Z}[x]$ be a separable polynomial (i.e. with no repeated roots) of positive degree. Assume that* $\gcd\{f(n) : n \in \mathbb{Z}\}$ *is square-free*[1] *. Then there are infinitely many square-free values taken by $f(n)$, in fact that a positive proportion of the values are square-free:*

$$\#\{1 \leq n \leq X : f(n) \text{ is square-free } \} \sim c_f X, \quad \text{as } X \to \infty ,$$

with

$$c_f = \prod_p (1 - \frac{\rho_f(p^2)}{p^2}) , \tag{1.1}$$

where

$$\rho_f(D) = \#\{c \bmod D : f(C) = 0 \bmod D\} . \tag{1.2}$$

The problem is most difficult when f is irreducible. Nagell ([6] 1922) showed the infinitude of squarefree values in the quadratic case. Estermann ([2] 1931) gave positive density for the case $f(x) = x^2 + k$. The general quadratic case was solved by Ricci in 1933 [7]. For cubics, Erdös ([1], 1953) showed that there are infinitely many square-free values, and Hooley ([4], 1967) gave the result about positive density. Beyond that nothing seems known unconditionally for irreducible f, for instance it is still not known that $a^4 + 2$ is infinitely often square-free.

Date: March 29, 2015.

[1] In fact one can even allow fixed, square divisors of $f(n)$, provided we divide them out in advance, by replacing $f(n)$ by $f(n)/B'$, where B' is the smallest divisor of $B := \gcd\{f(n) : n \in \mathbb{Z}\}$ so that B/B' is square-free, and if we replace c_f by $\prod_p (1 - \frac{\omega_f(p)}{p^{2+q_p}})$, where for each prime p, we denote by p^{q_p} the largest power of p dividing B', and by $\omega_f(p)$ the number of $a \bmod p^{2+q_p}$ for which $f(a)/B' = 0 \bmod p^2$.

A problem which has recently been solved is to ask how often an irreducible polynomial $f \in \mathbb{Z}[x]$ of degree d attains values which are free of $(d-1)$-th powers, either when evaluated at integers or at primes, see [8].

1.1. **The ABC conjecture.**

Granville [3] showed that the ABC conjecture completely solves the conjecture 1.

The ABC conjecture states that for every $\varepsilon > 0$, there exist only finitely many triples (a, b, c) of positive coprime integers, with $a + b = c$, such that

$$c > \operatorname{rad}(abc)^{1+\varepsilon} .$$

Here the radical of an integer is the product of all distinct primes dividing it: $\operatorname{rad}(N) := \prod_{p|N} p$. Equivalently, for every $\varepsilon > 0$, there exists a constant K_ε such that for all triples (a, b, c) of coprime positive integers, with $a + b = c$, we have

$$c < K_\varepsilon \cdot \operatorname{rad}(abc)^{1+\varepsilon} .$$

2. The density c_f

We pause to analyze the conjectural density c_f of squarefree values of f, given by (1.1).

Exercise 1. Assume that $f(n)$ admits no common square factor. Show that $c_f > 0$, i.e. that $\rho_f(p^2) < p^2$ for all primes p.

By the Chinese remainder theorem, $D \mapsto \rho_f(D)$ is a multiplicative function.

2.1. **The split quadratic case** $f(x) = x(x + 1)$**.**

Lemma 2.1. *Suppose $f(x) = x(x + 1)$. Then for all prime p, and $k \geq 1$, $\rho(p^k) = 2$.*

Proof. We want to count solutions modulo p^k of $c(c + 1) = 0 \bmod p^k$. But since p is prime, and c, $c+1$ have no common factors, this means that either $c = 0 \bmod p^k$ or $c + 1 = 0 \bmod p^k$ and each case has exactly one solution. Thus $\rho_f(p^k) = 2$. □

2.2. **The irreducible quadratic case** $f(x) = x^2 + 1$**.**

Lemma 2.2. *Suppose $f(x) = x^2 + 1$.*
i) If $p \neq 2$ then $\rho(p^k) = \rho(p)$ for all $k \geq 1$.
iii) For $p \neq 2$,

$$\rho(p) = \begin{cases} 2, & p = 1 \bmod 4 \\ 0, & p = 3 \bmod 4 \end{cases}$$

iii) $\rho(4) = 0$.

Proof. Part (i) follows from Hensel's Lemma, and is valid for any polynomial $f \in \mathbb{Z}[x]$, for $p \nmid \operatorname{disc}(f)$. Part (ii) is specific to $f(x) = x^2 + 1$ and is due to Fermat. Part (iii) is a direct computation. □

Note: The above shows that for $f(x) = x^2 + 1$, our density c_f is

$$c_f = \prod_p (1 - \frac{\rho(p^2)}{p^2}) = \prod_{p \neq 2} (1 - \frac{1 + \left(\frac{-1}{p}\right)}{p^2}) = 0.894\ldots \tag{2.1}$$

3. The quadratic case

Our goal here is to treat the quadratic case, in fact below we will specialize to the simple cases of $f(x) = x(x + 1)$ (the split case) and $f(x) = x^2 + 1$ (the irreducible case). For $X \gg 1$, we set

$$\mathcal{N}(X) := \{n \leq X : f(n) \text{ squarefree}\}$$

and $N(X) := \#\mathcal{N}(X)$.

Theorem 3.1. *Let $f(x) = x(x + 1)$ or $f(x) = x^2 + 1$. Then*

$$N(X) = c_f X + O(X^{2/3} \log X), \quad \text{as } X \to \infty$$

with $c_f = C_{\text{split}} = \prod_p (1 - \frac{2}{p^2})$ in the split case $f(x) = x(x + 1)$, and $c_f = \prod_{p \neq 2} (1 - \frac{1+(\frac{-1}{p})}{p^2}) = 0.894\ldots$ in the irreducible case $f(x) = x^2 + 1$.

Note that in the split case, since $n(n+1)$ is squarefree if and only if both n and $n + 1$ are squarefree (because n, $n + 1$ are coprime), the result says that the probability that both n and $n+1$ are squarefree is $C_{\text{split}} = \prod_p (1 - \frac{2}{p^2}) = 0.322635\ldots$, which is smaller than $1/\zeta(2)^2 = \prod_p (1 - 2/p^2 + 1/p^4) = 0.369576\ldots$, which would be the case if these were independent events.

3.1. The strategy.

We use the sieve of Eratosthenes and Legendre: Recall that the indicator function of the squarefrees is

$$\mathbf{1}_{\text{SF}}(m) = \sum_{d^2 | m} \mu(d) \ .$$

Hence

$$N(X) = \sum_{n \leq X} \mathbf{1}_{\text{SF}}(f(n)) = \sum_{n \leq X} \sum_{d^2 | f(n)} \mu(d) = \sum_{d \ll X} \mu(d) \#\{n \leq X : d^2 \mid f(n)\}$$

Note that we can constrain $d \leq X$ because d^2 divides the quadratic polynomial $f(n)$, which is $\ll X^2$ if $n \leq X$.

We pick a parameter Y (eventually taken to be $Y = X^{1/3}$) and decompose the sum into two parts, a sum $N'(X)$ over "small" divisors $d < Y$, and a sum $N''(X)$ over "large" divisors $Y < d < X$:

$$N(X) = N'(X) + N''(X) \ ,$$

$$N'(X) = \sum_{d \leq Y} \mu(d) \#\{n \leq X : d^2 \mid f(n)\}$$

and

$$N''(X) = \sum_{Y < d \leq X} \mu(d) \#\{n \leq X : d^2 \mid f(n)\}$$

We will show that

$$N'(X) = c_f X + O(\frac{X}{Y}\log Y + Y\log Y) \tag{3.1}$$

and

$$N''(X) \ll \frac{X^2}{Y^2} \tag{3.2}$$

Taking $Y = X^{1/3}$ we obtain

$$N(X) = c_f X + O(X^{2/3}\log X)$$

giving Theorem 3.1.

4. The main term: small divisors

We will estimate $N'(X)$ (the main term) by using inclusion-exclusion. Recall

$$N'(X) = \sum_{d\le Y} \mu(d)\#\{n \le X : d^2 \mid f(n)\} .$$

Lemma 4.1.

$$\#\{n \le X : D \mid f(n)\} = \frac{X\rho(D)}{D} + O\Big(\rho(D)\Big) .$$

Proof. We decompose

$$\#\{n \le X : D \mid f(n)\} = \sum_{\substack{C \bmod D \\ f(C)=0 \bmod D}} \#\{n \le X : n = C \bmod D\} .$$

Using

$$\#\{n \le X : n = C \bmod D\} = \frac{X}{D} + O(1)$$

we get

$$\begin{aligned} \#\{n \le X : D \mid f(n)\} &= \sum_{\substack{C \bmod D \\ f(C)=0 \bmod D}} \frac{X}{D} + O(1) \\ &= \frac{X\rho(D)}{D} + \rho(D) . \end{aligned}$$

□

Hence we obtain

$$\begin{aligned} N'(X) &= \sum_{d\le Y} \mu(d)\Big(\frac{X\rho(d^2)}{d^2} + O(\rho(d^2))\Big) \\ &= X\sum_{d\le Y} \frac{\mu(d)\rho(d^2)}{d^2} + O\Big(\sum_{d\le Y} |\mu(d)|\rho(d^2)\Big) . \end{aligned} \tag{4.1}$$

We have

$$\sum_{d\le Y}\frac{\mu(d)\rho(d^2)}{d^2}=\sum_{d=1}^{\infty}\frac{\mu(d)\rho(d^2)}{d^2}+O\Big(\sum_{d>Y}\frac{|\mu(d)|\rho(d^2)}{d^2}\Big)$$

Using multiplicativity of ρ (and of μ) gives

$$\sum_{d=1}^{\infty}\frac{\mu(d)\rho(d^2)}{d^2}=\prod_p(1-\frac{\rho(p^2)}{p^2})=c_f\ .$$

By Lemmas 2.1 and 2.2, $\rho(p^2)\le 2$ for p prime, and thus for d squarefree

$$\rho(d^2)=\prod_{p|d}\rho(p^2)\le\prod_{p|d}2=\tau(d)$$

where τ is the divisor function. Hence the tail of the sum is bounded by

$$\sum_{d>Y}\frac{|\mu(d)|\rho(d^2)}{d^2}\le\sum_{d>Y}\frac{\tau(d)}{d^2}\ll\frac{\log Y}{Y}$$

and the remainder in (4.1) is bounded by

$$\sum_{d\le Y}|\mu(d)|\rho(d^2)\le\sum_{d\le Y}\tau(d)\sim Y\log Y\ .$$

Therefore

$$N'(X)=c_fX+O(\frac{X}{Y}\log Y)+O(Y\log Y)$$

as claimed.

Exercise 2. Using $\sum_{n\le x}\tau(n)=x(\log x+C)+O(x^{1/2})$, show that

$$\sum_{n>Y}\frac{\tau(n)}{n^2}=\frac{\log Y+C+2}{Y}+O(\frac{1}{Y^{3/2}})$$

5. Bounding the contribution of large divisors

We write the condition $d^2\mid f(n)$ as $f(n)=d^2D$ for some integer $D\ge 1$. Then

$$N''(X)=\sum_{n\le X}\sum_{\substack{d^2|f(n)\\ d>Y}}\mu(d)\le\sum_{d>Y}\#\{n\le X: f(n)=d^2D\}\ .$$

We now interchange the roles of d and D: If $d>Y$ then $D=f(n)/d^2\le X^2/Y^2$. Hence ignoring the size and squarefreeness restriction on d,

$$N''(X)\le\sum_{1\le D\le X^2/Y^2}\#\{u,v\le X: f(u)=v^2D\}\ . \tag{5.1}$$

Now take $f(x)=x^2+1$. Then the equation $f(u)=Dv^2$ becomes

$$u^2-Dv^2=-1$$

which is a Pellian equation.

The main new arithmetic ingredient we need now is a bound on the number of solutions of the Pellian equation $x^2 - Dy^2 = -1$ lying in a box of side X: Let

$$S_D(X) := \#\{(x,y) \in [1,X]^2 : x^2 - Dy^2 = -1\} \tag{5.2}$$

Proposition 5.1. *Suppose $1 < D < X$ is not a perfect square. Then*

$$S_D(X) \ll \frac{\log X}{\log D} .$$

If $D = \square$ is a perfect square, then there are are no solutions of $x^2 - Dy^2 = -1$ if $D > 1$, while for $D = 1$ there are 2 solutions.

Proof. Suppose $D > 1$ is not a perfect square. By the theory of Pell's equation, if the equation $x^2 - Dy^2 = -1$ is solvable in integers, then all integer solutions (x,y) are of the form $x + \sqrt{D}y = \pm\epsilon_D^{2n+1}$, $n \in \mathbb{Z}$, where $\epsilon_D = x_1 + y_1\sqrt{D}$ is the fundamental solution, with $x_1, y_1 \geq 1$. Hence if $1 \leq x, y \leq X$ then $x + y\sqrt{D} = \epsilon_D^{2n+1}$ for some $n \geq 0$ and then

$$0 \leq n \leq \frac{\log(x + \sqrt{D}y)}{2\log\epsilon_D} = \frac{\log(x + \sqrt{x^2+1})}{2\log\epsilon_D} \leq \frac{\log X}{\log\epsilon_D} .$$

Since $\epsilon_D = x_1 + y_1\sqrt{D} > \sqrt{D}$, we obtain

$$S_D(X) \ll \frac{\log X}{\log D} .$$

For $D = C^2$ a perfect square, the equation $x^2 - Cy^2 = -1$ becomes $x^2 - (Cy)^2 = -1$ or $(Cy-x)(Cy+x) = 1$, which forces $Cy - x = Cy + x = \pm 1$, so that $x = 0$, and then $C^2y^2 = 1$ is solvable only for $C = 1$ in which case there are two solutions. $\square$

Inserting Proposition 5.1 into the bound (5.1) for N_2 gives

$$N_2 \ll \sum_{1 \leq D < X^2/Y^2} S_D(X) \ll 1 + \sum_{1 < D < X^2/Y^2} \frac{\log X}{\log D} \ll \frac{X^2}{Y^2}$$

as claimed, on using

$$\sum_{1<D<Z} \frac{1}{\log D} \ll \int_2^Z \frac{1}{\log t} dt \sim \frac{Z}{\log Z} .$$

5.1. **Other quadratic polynomials.** The considerations above extend to the case when $f(x) = Ax^2 + Bx + C \in \mathbb{Z}[x]$ is any quadratic polynomial, say $f(x) = x(x+1)$ (the split case). All we have to do is rewrite the equation $f(u) = Dv^2$: Multiplying by $4A$ and completing the square gives

$$4ADv^2 = (2Au + B)^2 - \Delta_f$$

where $\Delta_f = B^2 - 4AC$ is the discriminant of f, which is nonzero if and only if f has no repeated roots. Thus the equation $f(u) = Dv^2$ becomes

$$(2Au + B)^2 - AD(2v)^2 = \Delta_f$$

and we need to bound the number of solutions of

$$U^2 - (AD)V^2 = \Delta_f$$

with $U, V \ll X$.

For instance, in the split case $f(x) = x^2 + x$ we get $\Delta = +1$ and the equation becomes $U^2 - DV^2 = 1$, to which we apply a version of Proposition 5.1.

Remark. When $|\Delta| > 1$ there may be more than one orbit of the unit group $\{\pm\epsilon_D^n\}$ and one has to account for that.

References

[1] P. Erdös. *Arithmetical properties of polynomials.* J. London Math. Soc. 28, (1953). 416–425.

[2] T. Estermann, *Einige Sätze über quadratfreie Zahlen.* Math. Ann. 105 (1931), 653–662.

[3] A. Granville, *ABC allows us to count square-frees.* Internat. Math. Res. Notices 1998, no. 19, 991–1009.

[4] C. Hooley, *On the power free values of polynomials.* Mathematika 14 1967 21–26.

[5] C. Hooley, *On the square-free values of cubic polynomials.* Journal für die reine und angewandte Mathematik (Crelles Journal). (1968), 229, 147–154.

[6] T. Nagell, *Zur Arithmetik der Polynome*, Abhandl. Math. Sem. Hamburg 1 (1922), 179–194.

[7] G. Ricci, *Ricerche aritmetiche sui polinomi.* Rend. Circ. Mat. Palermo 57 (1933), 433–475.

[8] T. Reuss, *Power-Free Values of Polynomials*, Bull. London Math. Soc. (2015) doi: 10.1112/blms/bdu116. arXiv:1307.2802 [math.NT]