Binary expansions of values of quadratic forms

Alexander Kalmynin

Higher School of Economics, Moscow

Austrian-Russian online workshop
July 11-12, 2022

1. Introduction

Suppose that we have some interesting sequence a_n of natural numbers. What is the first most natural question one should ask about a_n in the context of analytic number theory?

1. Introduction

Suppose that we have some interesting sequence a_n of natural numbers. What is the first most natural question one should ask about a_n in the context of analytic number theory? Clearly, this most basic question is "what is the asymptotics of a_n?" or, equivalently, what is the asymptotics for

$$A(x) = \#\{n : a_n \leq x\}.$$

1. Introduction

Suppose that we have some interesting sequence a_n of natural numbers. What is the first most natural question one should ask about a_n in the context of analytic number theory? Clearly, this most basic question is "what is the asymptotics of a_n?" or, equivalently, what is the asymptotics for

$$A(x) = \#\{n : a_n \leq x\}.$$

For example, we all know the answer when $a_n = p_n$ is the $n-$th prime number and in this case it leads to more interesting questions on behavior of $\zeta(s)$. However, in this talk I am going to concentrate more on values of quadratic forms, so our most classical example would be the sequence s_n of all numbers that are sums of two squares.

1. Introduction

Suppose that we have some interesting sequence a_n of natural numbers. What is the first most natural question one should ask about a_n in the context of analytic number theory? Clearly, this most basic question is "what is the asymptotics of a_n?" or, equivalently, what is the asymptotics for

$$A(x) = \#\{n : a_n \leq x\}.$$

For example, we all know the answer when $a_n = p_n$ is the $n-$th prime number and in this case it leads to more interesting questions on behavior of $\zeta(s)$. However, in this talk I am going to concentrate more on values of quadratic forms, so our most classical example would be the sequence s_n of all numbers that are sums of two squares. In this case the answer to the first question is also well-known:

$$\#\{s_n \leq x\} \sim \frac{Kx}{\sqrt{\ln x}},$$

where

$$K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2} \approx 0.76422$$

1. Introduction

Okay, if we already know something about asymptotics of $A(x)$, what is the next natural question one should ask? Of course, there are lots of different candidates for a correct second question.

Okay, if we already know something about asymptotics of $A(x)$, what is the next natural question one should ask? Of course, there are lots of different candidates for a correct second question. My favourite option is the problem of estimating gaps, i.e. the function

$$G_a(x) = \max_{a_{n+1} \le x} (a_{n+1} - a_n).$$

1. Introduction

Okay, if we already know something about asymptotics of $A(x)$, what is the next natural question one should ask? Of course, there are lots of different candidates for a correct second question. My favourite option is the problem of estimating gaps, i.e. the function

$$G_a(x) = \max_{a_{n+1} \leq x} (a_{n+1} - a_n).$$

This problem, however, sometimes turns out to be extremely difficult. For example, for our example above, $a_n = s_n$, it is known that

$$G_s(x) \ll x^{1/4}.$$

Okay, if we already know something about asymptotics of $A(x)$, what is the next natural question one should ask? Of course, there are lots of different candidates for a correct second question. My favourite option is the problem of estimating gaps, i.e. the function

$$G_a(x) = \max_{a_{n+1} \le x} (a_{n+1} - a_n).$$

This problem, however, sometimes turns out to be extremely difficult. For example, for our example above, $a_n = s_n$, it is known that

$$G_s(x) \ll x^{1/4}.$$

The proof is completely obvious: one can approximate any number below x by a square from below with an error $O(\sqrt{x})$, do this two times and you get this estimate. Interestingly, this result is still the best known.

As for the lower bounds for $G_s(x)$, they are constructive in nature. More precisely, proofs take $X \asymp \ln x$ and construct some nice residue modulo

$$P = 4 \prod_{p \equiv 3 \pmod 4, p \leq X} p^{[\ln X/\ln p]+1}.$$

1. Introduction

As for the lower bounds for $G_s(x)$, they are constructive in nature. More precisely, proofs take $X \asymp \ln x$ and construct some nice residue modulo

$$P = 4 \prod_{p \equiv 3 \pmod 4, p \leq X} p^{[\ln X / \ln p]+1}.$$

For example, a result of P. Erdős (1951) gives

$$G_s(x) \gg \frac{\ln x}{\sqrt{\ln \ln x}}$$

and result of I. Richards (1982) states that

$$G_s(x) \geq \left(\frac{1}{4} + o(1)\right) \ln x.$$

This was recently improved by R. Dietmann, C. Elsholtz, A.K., S. Konyagin and J. Maynard to $\left(\frac{390}{449} + o(1)\right) \ln x$.

2. The third question

During my visit in Austria in 2019, C. Elsholtz told me about a third kind of question one can ask about a sequence. Namely, can one construct values of a_n with anomalous binary expansions?

2. The third question

During my visit in Austria in 2019, C. Elsholtz told me about a third kind of question one can ask about a sequence. Namely, can one construct values of a_n with anomalous binary expansions? His question was more particular: given $\varepsilon > 0$, can we prove that there are sums of two squares with proportion of ones in binary expansion at least $1 - \varepsilon$? Clearly, analogous question for zeroes is trivial, since all powers of 2 are sums of two squares.

2. The third question

During my visit in Austria in 2019, C. Elsholtz told me about a third kind of question one can ask about a sequence. Namely, can one construct values of a_n with anomalous binary expansions? His question was more particular: given $\varepsilon > 0$, can we prove that there are sums of two squares with proportion of ones in binary expansion at least $1-\varepsilon$? Clearly, analogous question for zeroes is trivial, since all powers of 2 are sums of two squares. Let us discuss several approaches to this problem. First of all, we can emulate the proof of the bound $G_s(x) \ll x^{1/4}$ and notice that

$$(2^{2n-1}-1)^2+(2^n-1)^2 = 2^{4n-2}-2^{2n}+1+2^{2n}-2^{n+1}+1 = 2^{4n-2}-2^{n+1}+2.$$

This number has $4n+O(1)$ digits and $3n+O(1)$ of them are equal to 1, so we get $\varepsilon = 1/4 - o(1)$.

2. The third question

During my visit in Austria in 2019, C. Elsholtz told me about a third kind of question one can ask about a sequence. Namely, can one construct values of a_n with anomalous binary expansions? His question was more particular: given $\varepsilon > 0$, can we prove that there are sums of two squares with proportion of ones in binary expansion at least $1 - \varepsilon$? Clearly, analogous question for zeroes is trivial, since all powers of 2 are sums of two squares. Let us discuss several approaches to this problem. First of all, we can emulate the proof of the bound $G_s(x) \ll x^{1/4}$ and notice that

$$(2^{2n-1}-1)^2+(2^n-1)^2 = 2^{4n-2}-2^{2n}+1+2^{2n}-2^{n+1}+1 = 2^{4n-2}-2^{n+1}+2.$$

This number has $4n + O(1)$ digits and $3n + O(1)$ of them are equal to 1, so we get $\varepsilon = 1/4 - o(1)$. Curiously, in this context one can use current results on Gauss circle problem to achieve a somewhat better proportion.

2. The third question

More precisely, M. Huxley proved that if $r_2(n)$ is the number of representations of n as a sum of two squares, then

$$\sum_{n \le x} r_2(n) = \pi x + O(x^{131/416+o(1)}).$$

2. The third question

More precisely, M. Huxley proved that if $r_2(n)$ is the number of representations of n as a sum of two squares, then

$$\sum_{n \leq x} r_2(n) = \pi x + O(x^{131/416+o(1)}).$$

Since $r_2(n) \ll n^{o(1)}$, this implies, for instance, that for $n \to +\infty$ and $b > 131/416$ there are $2^{bn-o(n)}$ sums of two squares between $2^n - 2^{bn}$ and $2^n - 1$. All numbers N in this interval have binary expansions of the form

$$N = \underbrace{11\ldots1}_{head}\underbrace{\varepsilon_1\ldots\varepsilon_{bn}}_{tail}$$

Here "head" has $\approx n(1-b)$ ones and "tail" has $\approx nb$ random digits. Simple application of, say, central limit theorem, shows that for all but $2^{(b-\varepsilon)n}$ numbers the tail contains at least $nb(1/2-\delta)$ ones.

2. The third question

More precisely, M. Huxley proved that if $r_2(n)$ is the number of representations of n as a sum of two squares, then

$$\sum_{n \le x} r_2(n) = \pi x + O(x^{131/416+o(1)}).$$

Since $r_2(n) \ll n^{o(1)}$, this implies, for instance, that for $n \to +\infty$ and $b > 131/416$ there are $2^{bn-o(n)}$ sums of two squares between $2^n - 2^{bn}$ and $2^n - 1$. All numbers N in this interval have binary expansions of the form

$$N = \underbrace{11\ldots1}_{head}\underbrace{\varepsilon_1\ldots\varepsilon_{bn}}_{tail}$$

Here "head" has $\approx n(1-b)$ ones and "tail" has $\approx nb$ random digits. Simple application of, say, central limit theorem, shows that for all but $2^{(b-\varepsilon)n}$ numbers the tail contains at least $nb(1/2-\delta)$ ones. This approach gives the proportion $1 - b + b/2 + o(1) = (2-b)/2 + o(1)$, i.e. for $b \to 131/416$ we obtain the proportion $701/832 - o(1)$, i.e. $\varepsilon = \frac{131}{832} \approx 0.15745$

2. The third question

It turns out, however, that one can construct sums of two squares with a lot of 1's explicitly without any theorems on Gauss circle problem!

2. The third question

It turns out, however, that one can construct sums of two squares with a lot of 1's explicitly without any theorems on Gauss circle problem!

Theorem 1

For any $n \geq 1$ the number $3(2^{2^n} - 1)$ is a sum of two squares. Also, it has only two zeros in binary expansion.

The second part is easy to see:
$3(2^{2^n} - 1) = 2^{2^n+1} + 2^{2^n} - 3 = 2^{2^n+1} + 2^{2^n-1} + 2^{2^n-2} + \ldots + 2^2 + 1.$

2. The third question

It turns out, however, that one can construct sums of two squares with a lot of 1's explicitly without any theorems on Gauss circle problem!

Theorem 1

For any $n \geq 1$ the number $3(2^{2^n} - 1)$ is a sum of two squares. Also, it has only two zeros in binary expansion.

The second part is easy to see:
$3(2^{2^n} - 1) = 2^{2^n+1} + 2^{2^n} - 3 = 2^{2^n+1} + 2^{2^n-1} + 2^{2^n-2} + \ldots + 2^2 + 1$.
As for the first part, notice that $2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1)$.
Applying this formula repeatedly, we get

$$3(2^{2^n}-1) = 3(2^{2^{n-1}}+1)(2^{2^{n-1}}-1) = 3(2^{2^{n-1}}+1)(2^{2^{n-2}}+1)\ldots(2^2+1)(2+1).$$

This product contains only factors of the form $x^2 + 1$ and also first and last factors, which both are equal to 3. Since sums of two squares are multiplicatively closed, we get the desired result.

2. The third question

It feels that Theorem 1 should have a generalization to other quadratic forms. Let us discuss such a generalization.

2. The third question

It feels that Theorem 1 should have a generalization to other quadratic forms. Let us discuss such a generalization.

Theorem 2

Let $D \neq 1$ be a fundamental discriminant, i.e. either D is squarefree and $D \equiv 1 \pmod 4$ or $D/4$ is squarefree and $D/4 \equiv 2$ or $3 \pmod 4$. Then for any quadratic form $Q(x,y) = Ax^2 + Bxy + Cy^2$ with $B^2 - 4AC = D$ and any $\varepsilon > 0$ there are infinitely many values x, y such that $Q(x,y)$ has proportion of ones in binary expansion at least $1 - \varepsilon$.

2. The third question

It feels that Theorem 1 should have a generalization to other quadratic forms. Let us discuss such a generalization.

Theorem 2

Let $D \neq 1$ be a fundamental discriminant, i.e. either D is squarefree and $D \equiv 1 \pmod 4$ or $D/4$ is squarefree and $D/4 \equiv 2$ or $3 \pmod 4$. Then for any quadratic form $Q(x,y) = Ax^2 + Bxy + Cy^2$ with $B^2 - 4AC = D$ and any $\varepsilon > 0$ there are infinitely many values x, y such that $Q(x,y)$ has proportion of ones in binary expansion at least $1 - \varepsilon$.

To prove this, notice first that it is enough to find a large number N with large proportion of ones in binary expansion, represented by *some* quadratic form of discriminant D. Indeed, by Gauss composition law, for any two quadratic forms Q_1, Q_2 of discriminant D there is a quadratic form Q_3 such that for all x_1, y_1, x_2, y_2 there are x_3, y_3 with $Q_1(x_1, y_1)Q_2(x_2, y_2) = Q_3(x_3, y_3)$.

2. The third question

It feels that Theorem 1 should have a generalization to other quadratic forms. Let us discuss such a generalization.

Theorem 2

Let $D \neq 1$ be a fundamental discriminant, i.e. either D is squarefree and $D \equiv 1 \pmod 4$ or $D/4$ is squarefree and $D/4 \equiv 2$ or $3 \pmod 4$. Then for any quadratic form $Q(x,y) = Ax^2 + Bxy + Cy^2$ with $B^2 - 4AC = D$ and any $\varepsilon > 0$ there are infinitely many values x, y such that $Q(x,y)$ has proportion of ones in binary expansion at least $1 - \varepsilon$.

To prove this, notice first that it is enough to find a large number N with large proportion of ones in binary expansion, represented by *some* quadratic form of discriminant D. Indeed, by Gauss composition law, for any two quadratic forms Q_1, Q_2 of discriminant D there is a quadratic form Q_3 such that for all x_1, y_1, x_2, y_2 there are x_3, y_3 with $Q_1(x_1,y_1)Q_2(x_2,y_2) = Q_3(x_3,y_3)$. The set of $SL(2,\mathbb{Z})-$equivalence classes of quadratic forms is a finite abelian group with respect to this operation.

2. The third question

Therefore, one can find a finite set of non-zero integers $a_1, \ldots, a_h$ such that if $N = Q(x,y)$ and Q_1 is a quadratic form of discriminant D then for some $i \le h$ we have $a_i N = Q_1(X,Y)$.

2. The third question

Therefore, one can find a finite set of non-zero integers $a_1, \ldots, a_h$ such that if $N = Q(x, y)$ and Q_1 is a quadratic form of discriminant D then for some $i \leq h$ we have $a_i N = Q_1(X, Y)$. This proves the claim above, since if N has few zeros in binary expansion, then so does $a_i N$. First of all, let us figure out the case of prime $|D|$.

2. The third question

Therefore, one can find a finite set of non-zero integers $a_1, \dots, a_h$ such that if $N = Q(x, y)$ and Q_1 is a quadratic form of discriminant D then for some $i \le h$ we have $a_i N = Q_1(X, Y)$. This proves the claim above, since if N has few zeros in binary expansion, then so does $a_i N$. First of all, let us figure out the case of prime $|D|$. The case $D > 0$ is trivial, so we are only interested in $D = -p$, where $p \equiv 3 \pmod 4$. In this case, we have the following:

Lemma 1

Let $p \equiv 3 \pmod 4$ be a prime, $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ be the cyclotomic polynomial. Then there are polynomials $A_p(x)$ and $B_p(x)$ with

$$\Phi_p(x) = A_p^2(x) + A_p(x)B_p(x) + \frac{p+1}{4}B_p(x)^2.$$

Therefore, one can find a finite set of non-zero integers $a_1, \ldots, a_h$ such that if $N = Q(x, y)$ and Q_1 is a quadratic form of discriminant D then for some $i \le h$ we have $a_i N = Q_1(X, Y)$. This proves the claim above, since if N has few zeros in binary expansion, then so does $a_i N$. First of all, let us figure out the case of prime $|D|$. The case $D > 0$ is trivial, so we are only interested in $D = -p$, where $p \equiv 3 \pmod 4$. In this case, we have the following:

Lemma 1

Let $p \equiv 3 \pmod 4$ be a prime, $\Phi_p(x) = \frac{x^p - 1}{x - 1}$ be the cyclotomic polynomial. Then there are polynomials $A_p(x)$ and $B_p(x)$ with

$$\Phi_p(x) = A_p^2(x) + A_p(x)B_p(x) + \frac{p+1}{4} B_p(x)^2.$$

To see this, take $\zeta_p = \exp\left(\frac{2\pi i}{p}\right)$ and consider $\mathbb{Z}[\zeta_p]$. The polynomial $\Phi_p(x)$ factors into linear factors over this ring.

2. The third question

Next, the Gauss sum gives you an inclusion $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \subset \mathbb{Z}[\zeta_p]$. Factorization of $\Phi_p(x)$ also gives a formula $\Phi_p(x) = C_p(x)\overline{C_p}(x)$, where $C_p \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\overline{C_p}$ is a polynomial with conjugate coefficients.

2. The third question

Next, the Gauss sum gives you an inclusion $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \subset \mathbb{Z}[\zeta_p]$. Factorization of $\Phi_p(x)$ also gives a formula $\Phi_p(x) = C_p(x)\overline{C_p}(x)$, where $C_p \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\overline{C_p}$ is a polynomial with conjugate coefficients. This concludes the proof. For example, explicit computations show that

$$(x^3-x-1)^2+(x^3-x-1)(x^2+x)+2(x^2+x)^2 = x^6+x^5+\ldots+1 = \Phi_7(x).$$

Next, the Gauss sum gives you an inclusion $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \subset \mathbb{Z}[\zeta_p]$. Factorization of $\Phi_p(x)$ also gives a formula $\Phi_p(x) = C_p(x)\overline{C_p}(x)$, where $C_p \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\overline{C_p}$ is a polynomial with conjugate coefficients. This concludes the proof. For example, explicit computations show that

$$(x^3-x-1)^2+(x^3-x-1)(x^2+x)+2(x^2+x)^2 = x^6+x^5+\ldots+1 = \Phi_7(x).$$

Taking large k and considering

$$f_k(x) = \Phi_p(x)\Phi_p(x^p)\ldots\Phi_p(x^{p^{k-1}})$$

we notice that by Lemma 1 all values of $f_k(x)$ are represented by $X^2 + XY + \frac{p+1}{4}Y^2$.

2. The third question

Next, the Gauss sum gives you an inclusion $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right] \subset \mathbb{Z}[\zeta_p]$. Factorization of $\Phi_p(x)$ also gives a formula $\Phi_p(x) = C_p(x)\overline{C_p}(x)$, where $C_p \in \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ and $\overline{C_p}$ is a polynomial with conjugate coefficients. This concludes the proof. For example, explicit computations show that

$$(x^3-x-1)^2+(x^3-x-1)(x^2+x)+2(x^2+x)^2 = x^6+x^5+\ldots+1 = \Phi_7(x).$$

Taking large k and considering

$$f_k(x) = \Phi_p(x)\Phi_p(x^p)\ldots\Phi_p(x^{p^{k-1}})$$

we notice that by Lemma 1 all values of $f_k(x)$ are represented by $X^2 + XY + \frac{p+1}{4}Y^2$. On the other hand,

$$\Phi_p(x)\Phi_p(x^p)\ldots\Phi_p(x^{p^{k-1}}) = \frac{x^p-1}{x-1}\frac{x^{p^2}-1}{x^p-1}\ldots\frac{x^{p^k}-1}{x^{p^{k-1}}-1} = \frac{x^{p^k}-1}{x-1}.$$

2. The third question

This means that $f_k(2) = 2^{p^k} - 1$ is always represented by $x^2 + xy + \frac{p+1}{4}y^2$, which concludes the proof for prime $|D|$. For example, we get

$$2^{343} - 1 = x^2 + xy + 2y^2$$

for

$$x = 42207992669249423822778381183318245559940690891137 55$$

and

$$y = 24083462164432519803208981310273770299704201178234.$$

2. The third question

This means that $f_k(2) = 2^{p^k} - 1$ is always represented by $x^2 + xy + \frac{p+1}{4}y^2$, which concludes the proof for prime $|D|$. For example, we get

$$2^{343} - 1 = x^2 + xy + 2y^2$$

for

$$x = 4220799266924942382277838118331824555994069089113755$$

and

$$y = 2408346216443251980320898131027377029970420117823 4.$$

How do we generalize such a proof? For simplicity, let us assume that D is odd. One can notice that a number N is represented by some quadratic form of discriminant D iff there is no odd α and prime p with $\left(\frac{D}{p}\right) = -1$ and $p^\alpha \mid\mid N$. One can prove this, for example, using the factorization of Dedekind zeta-function of $\mathbb{Q}(\sqrt{D})$:

$$\zeta_{\mathbb{Q}(\sqrt{D})}(s) = \zeta(s)L(s, \chi_D)$$

2. The third question

On the other hand, all prime factors of $\Phi_{|D|}(x)$ for even x are either prime factors of $|D|$ or of the form $|D|k+1$. This, together with the quadratic reciprocity law, proves that values of $\Phi_{|D|}(x)$ are always represented by some quadratic form of discriminant D (much more explicit results are known).

On the other hand, all prime factors of $\Phi_{|D|}(x)$ for even x are either prime factors of $|D|$ or of the form $|D|k+1$. This, together with the quadratic reciprocity law, proves that values of $\Phi_{|D|}(x)$ are always represented by some quadratic form of discriminant D (much more explicit results are known). Therefore, we can always take products of some numbers of the form $\Phi_{|D|}(2^d)$. The trick is to make the resulting number have few zeros in the binary expansion. To do so, notice first that

$$\Phi_{|D|}(x) = \prod_{d||D|} (x^d - 1)^{\mu(|D|/d)}.$$

Möbius inversion then gives

$$\Phi^{(2)}_{|D|}(x) := \prod_{d||D|} \Phi_{|D|}(x^d) = \prod_{d||D|} (x^{d^2} - 1)^{\mu(|D|/d)}.$$

2. The third question

On the other hand, all prime factors of $\Phi_{|D|}(x)$ for even x are either prime factors of $|D|$ or of the form $|D|k+1$. This, together with the quadratic reciprocity law, proves that values of $\Phi_{|D|}(x)$ are always represented by some quadratic form of discriminant D (much more explicit results are known). Therefore, we can always take products of some numbers of the form $\Phi_{|D|}(2^d)$. The trick is to make the resulting number have few zeros in the binary expansion. To do so, notice first that

$$\Phi_{|D|}(x) = \prod_{d||D|} (x^d - 1)^{\mu(|D|/d)}.$$

Möbius inversion then gives

$$\Phi^{(2)}_{|D|}(x) := \prod_{d||D|} \Phi_{|D|}(x^d) = \prod_{d||D|} (x^{d^2} - 1)^{\mu(|D|/d)}.$$

Continuing this process, we can set

$$\Phi^{(k)}_{|D|}(x) = \prod_{d||D|} \Phi^{(k-1)}_{|D|}(x^{d^{2^{k-1}}})$$

2. The third question

We then obtain

$$\Phi_{|D|}^{(k)}(x) = \prod_{d||D|} (x^{d^{2^k}} - 1)^{\mu(|D|/d)}.$$

We then obtain

$$\Phi_{|D|}^{(k)}(x) = \prod_{d||D|} (x^{d^{2^k}} - 1)^{\mu(|D|/d)}.$$

When k is large, this expansion has a clear dominating term: $x^{|D|^{2^k}} - 1$. To obtain our result we now need to get rid of the "denominator":

$$\prod_{d|||D|:\mu(|D|/d)=-1} (x^{d^{2^k}} - 1)^2 \Phi_{|D|}^{(k)}(x) = \prod_{d||D|} (x^{d^{2^k}} - 1)^{\mu^2(|D|/d)}.$$

2. The third question

We then obtain

$$\Phi^{(k)}_{|D|}(x) = \prod_{d||D|} (x^{d^{2^k}} - 1)^{\mu(|D|/d)}.$$

When k is large, this expansion has a clear dominating term: $x^{|D|^{2^k}} - 1$. To obtain our result we now need to get rid of the "denominator":

$$\prod_{d|||D|:\mu(|D|/d)=-1} (x^{d^{2^k}} - 1)^2 \Phi^{(k)}_{|D|}(x) = \prod_{d||D|} (x^{d^{2^k}} - 1)^{\mu^2(|D|/d)}.$$

Since this last operation cannot produce any odd exponents in factorization, we see that the number

$$\prod_{d||D|} (2^{d^{2^k}} - 1)^{\mu^2(|D|/d)}$$

is always represented by some quadratic form of discriminant $|D|$.

2. The third question

On the other hand, if we denote the product without $d = |D|$ term by N, i.e.

$$N = \prod_{d||D|, d \neq |D|} (2^{d^{2^k}} - 1)^{\mu^2(|D|/d)},$$

then for $k \to +\infty$ we have $N \ll 2^{o(|D|^{2^k})}$.

On the other hand, if we denote the product without $d = |D|$ term by N, i.e.

$$N = \prod_{d||D|, d \neq |D|} (2^{d^{2^k}} - 1)^{\mu^2(|D|/d)},$$

then for $k \to +\infty$ we have $N \ll 2^{o(|D|^{2^k})}$. If we set $A = N(2^{|D|^{2^k}} - 1)$ and $B = N - 1$, then for the binary digit sums s_2 we get from subadditivity

$$|D|^{2^k} \leq s_2(N2^{|D|^{2^k}} - 1) = s_2(A+B) \leq s_2(A) + s_2(B) = s_2(A) + o(|D|^{2^k}),$$

which concludes the proof.

3. Conclusion

The content of this talk gives several answers to “the third question” for quadratic forms, but it also raises several more questions. For instance, one can notice that for sums of two squares we produced an example which is always divisible by 9, hence its representation is never primitive. Can we give an example with a primitive representation?

3. Conclusion

The content of this talk gives several answers to "the third question" for quadratic forms, but it also raises several more questions. For instance, one can notice that for sums of two squares we produced an example which is always divisible by 9, hence its representation is never primitive. Can we give an example with a primitive representation? Same question arises for some values of $|D|$, since we multiplied by some square at the end.

3. Conclusion

The content of this talk gives several answers to "the third question" for quadratic forms, but it also raises several more questions. For instance, one can notice that for sums of two squares we produced an example which is always divisible by 9, hence its representation is never primitive. Can we give an example with a primitive representation? Same question arises for some values of $|D|$, since we multiplied by some square at the end. Also, our proof gives a number with N digits and $O(N^a)$ zeros for some $a < 1$. Can we always replace it by $O(1)$, like in the case of two squares?

The content of this talk gives several answers to "the third question" for quadratic forms, but it also raises several more questions. For instance, one can notice that for sums of two squares we produced an example which is always divisible by 9, hence its representation is never primitive. Can we give an example with a primitive representation? Same question arises for some values of $|D|$, since we multiplied by some square at the end. Also, our proof gives a number with N digits and $O(N^a)$ zeros for some $a < 1$. Can we always replace it by $O(1)$, like in the case of two squares? During some discussion on this topic, S.V. Konyagin also asked what can be done for squarefree integers. I gave this problem as a Master's thesis topic to my student K. Bobkov.

3. Conclusion

For squarefree integers, recent result by Tsz Ho Chan states that the interval $(x, x+Cx^{5/26})$ always contains a lot of squarefree numbers. Therefore, the "trivial" proportion in this case is $\frac{2-5/26}{2} - o(1) = \frac{47}{52} - o(1)$ — a bit larger than 90%.

3. Conclusion

For squarefree integers, recent result by Tsz Ho Chan states that the interval $(x, x + Cx^{5/26})$ always contains a lot of squarefree numbers. Therefore, the "trivial" proportion in this case is $\frac{2-5/26}{2} - o(1) = \frac{47}{52} - o(1)$ — a bit larger than 90%. Unfortunately, improving this seems to be difficult. Konstantin was able to improve upon the "trivial" exponent for the case of k-free numbers. For k-free numbers, the trivial exponent turns out to be $1 - \frac{1}{4k+2}$.

3. Conclusion

For squarefree integers, recent result by Tsz Ho Chan states that the interval $(x, x + Cx^{5/26})$ always contains a lot of squarefree numbers. Therefore, the "trivial" proportion in this case is $\frac{2-5/26}{2} - o(1) = \frac{47}{52} - o(1)$ — a bit larger than 90%. Unfortunately, improving this seems to be difficult. Konstantin was able to improve upon the "trivial" exponent for the case of k-free numbers. For k-free numbers, the trivial exponent turns out to be $1 - \frac{1}{4k+2}$. Using results on moments of gaps between k-free numbers, K. Bobkov was able to prove the following result:

Theorem 3 (K. Bobkov, 2022)

For large k, for any $\alpha < 1 - \frac{2 \ln 2}{k \ln k}$ there are infinitely many k-free numbers with the proportion of ones in binary expansion greater than α.

3. Conclusion

This result becomes better than the trivial one for $k > 258$. Two natural questions here are: "what happens for $k \le 258$?" and "can we do better than $O\left(\frac{1}{k \ln k}\right)$?".

3. Conclusion

This result becomes better than the trivial one for $k > 258$. Two natural questions here are: "what happens for $k \leq 258$?" and "can we do better than $O\left(\frac{1}{k \ln k}\right)$?". I would hope to improve $1/k \ln k$ to k^{-1-c} for some $c > 0$.

Thank you for your attention!