Asymptotics of the number of $D(q)$-pairs and $D(q)$-triples via L-functions

Nikola Adžaga

Representation Theory XVIII

Dubrovnik, 22 Jun 2023

Joint work with Dražić, Dujella and Pethő.

This work has been supported in part by the Croatian Science Foundation.

Definitions

Fix a nonzero integer q. A $D(q)$-*pair* is a pair $\{a, b\}$ of positive integers such that $ab + q = \square$.

How many pairs are such that $a < b \leqslant N$? Denote

$$D_q(N) := D_{2,q}(N) := \text{the number of } D(q)\text{-pairs up to N.}$$

If $ab + q = x^2$, then $a = \frac{x^2-q}{b}$, i. e.

$$x^2 \equiv q \pmod{b}.$$

Reducing the problem to congruences

$$x^2 \equiv q \pmod{b} \tag{1}$$

Almost all solutions of (1) such that $x \leqslant b$ induce a $D(q)$-pair by setting $a = \frac{x^2-q}{b}$ (there are at most $O(\sqrt{q})$ solutions giving a negative a – even if b varies).

If $a < b \leqslant N$ form a $D(q)$-pair such that $a > \frac{x^2-q}{b}$ for all solutions of (1) with $x \leqslant b$, then

$$b > a \geqslant \frac{(b+1)^2 - q}{b} \implies b \leqslant \frac{q-1}{2}.$$

Essentially, we count solutions $x \in \{1, 2, \ldots, b\}$ of (1) where b runs up to N.

Counting solutions of congruences

Fix a nonzero integer q. Let b vary from 1 to N. How many solutions $x \in \{1, 2, \ldots, b\}$ of

$$x^2 \equiv q \pmod{b},$$

in total, are there?

Previous results I

For $q = 1$, Duje (2008) found that

$$D_{2,1}(N) = \frac{6}{\pi^2} N \log N + O(N).$$

Lao (2010) found the error term.

A $D(q)$-m-tuple is a set $\{a_1, a_2, \ldots, a_m\}$ of positive integers such that $a_i a_j + q = \square$ for all $1 \leqslant i < j \leqslant m$.
Denote by $D_{3,q}$ the number of $D(q)$-triples up to N, and by $D_{4,q}$ the number of $D(q)$-quadruples up to N.

Previous results II

For $q = 1$, Duje has also shown that

$$D_{3,1}(N) = \frac{3}{\pi^2} N \log N + O(N),$$

and that the true order of magnitude of $D_{4,1}(N)$ is $\sqrt[3]{N} \log N$.

Martin and Sitar (2011) have then shown that

$$D_{4,1}(N) \sim \frac{2^{4/3}}{3\Gamma(2/3)^3} \sqrt[3]{N} \log N.$$

So far, infinitely many $D(q)$-quadruples have been found only for square numbers q.

Our results I

Theorem 1 (A.-Dražić-Dujella-Pethő, 2023+)

The number of $D(2)$-pairs up to N satisfies

$$D_{2,2}(N) \sim \frac{L(1, \chi_{8,5})}{\zeta(2)} \cdot N \approx 0.37888N,$$

whereas the number of $D(-2)$-pairs with both elements in the set $\{1, 2, \ldots, N\}$ satisfies

$$D_{2,-2}(N) \sim \frac{L(1, \chi_{8,3})}{\zeta(2)} \cdot N \approx 0.67524N.$$

The results for other primes q depend on the remainder of q modulo 8 (i. e. on the power of 2 dividing $q - 1$).

Our results II

Theorem 2 (A.-Dražić-Dujella-Pethő, 2023+)

Let q be an integer such that $|q|$ is a prime or $q = -1$.

a) *If $q \equiv 3 \pmod 4$, then*

$$D_{2,q}(N) \sim \frac{L(1, \chi_{4|q|,4|q|-1})}{\zeta(2)} \cdot N.$$

b) *If $q \equiv 5 \pmod 8$, then*

$$D_{2,q}(N) \sim \frac{2L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

c) *If $q \equiv 1 \pmod 8$, then*

$$D_{2,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

Our results III

Theorem 3 (A.-Dražić-Dujella-Pethő, 2023+)

Let n be a non-zero integer. The number of $D(n)$-triples with all elements in the set $\{1, 2, \ldots, N\}$ is asymptotically equal to half the number of $D(n)$-pairs:

$$D_{3,n}(N) \sim \frac{D_{2,n}(N)}{2}.$$

Number of congruence solutions (with fixed modulus)

Let $\omega(n)$ denote the number of distinct prime factors of n.

Lemma 4

Let q be an odd prime and $b \in \mathbb{N}$ such that $\gcd(b, 2q) = 1$. Then the number of solutions of the congruence

$$x^2 \equiv 1 \pmod{b} \tag{2}$$

such that $1 \leqslant x \leqslant b$ is $2^{\omega(b)}$. Consequently, the number of solutions x of the congruence

$$x^2 \equiv q \pmod{b} \tag{1}$$

such that $1 \leqslant x \leqslant b$ is either zero or $2^{\omega(b)}$.

Proof of lemma

Proof.

If there is no solution to Equation (1), we are done. If there exists a solution x_q, then every other solution x' satisfies

$$\left(\frac{x'}{x_q}\right)^2 \equiv 1 \pmod{b}.$$

Also, if x_1 is any solution to Equation (2), then $x_1 x_q$ is a solution of Equation (1) and all solutions obtained in such a way have different residues mod b. □

Similarity with Duje's proof

For D(1)-pairs, the problem is reduced to estimating the sum

$$\sum_{n=1}^{N} 2^{\omega(n)}.$$

For D(q)-pairs, we have to estimate a weighted version of this sum. The weights are binary, depending on whether the congruence $x^2 \equiv q \pmod{n}$ is soluble.

Is the congruence soluble? (Ex. $q = 3$)

Whether

$$x^2 \equiv 3 \pmod{n}$$

has solutions or not depends on the prime factors of n. The first observation is that 2 and 3 can divide n at most once. For other primes p, we can look at their Legendre symbol modulo $q = 3$.

Lemma 5

Let prime $q = 3 \pmod{4}$. Equation (1) has a solution if and only if $b = \delta \prod_{p_i \neq q} p_i^{\alpha_i}$ such that $\left(\frac{q}{p_i}\right) = 1$ for all i, and $\delta \in \{1, 2, q = 3, 2q = 6\}$. The condition $\left(\frac{q}{p_i}\right) = 1$ is equivalent to $\left(\frac{p_i}{q}\right) = (-1)^{\frac{p_i - 1}{2}}$.

Good primes

The previous lemma motivates the following definition. We call a prime p *good for q* if $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}}$.

Sketch of proof (of lemma):

- powers of 2 and q.
- quadratic reciprocity for each prime $p|n$.
- if n is composed of "good" primes then there exists a solution (Hensel lemma argument).

For $q = 3$, the set of good primes is

$$\mathcal{G}_3 = \{p \equiv \pm 1 \pmod{12}\}.$$

The number of solutions

Lemma 6

(Extension of Lemma 4) Let $b \in \mathbb{N}$ *such that* $\gcd(b, 2q) = 1$, *and* b *has only good prime factors for* $q \equiv 3 \pmod 4$. *The following table gives the number of solutions of the congruence equation*

equation	*interval*	*the number of solutions*
$x^2 \equiv q \pmod{2b}$	$1 \leqslant x \leqslant 2b$	$2^{\omega(2b)-1}$
$x^2 \equiv q \pmod{qb}$	$1 \leqslant x \leqslant qb$	$2^{\omega(qb)-1}$
$x^2 \equiv q \pmod{2qb}$	$1 \leqslant x \leqslant 2qb$	$2^{\omega(2qb)-2}$

Accompanying arithmetic functions

$$\mathcal{G} = \mathcal{G}_3 = \{p \equiv \pm 1 \pmod{12}\}.$$

Let

$$\lambda_{\mathcal{G}}(n) = \begin{cases} 1, & \text{if } n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad p_i \in \mathcal{G} \\ 0, & \text{otherwise} \end{cases},$$

along with

$$b_3(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n).$$

The weighted sum

We want to estimate

$$B_3(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) = \sum_{1 \leqslant n \leqslant N} b_3(n).$$

$B_3(N)$ counts the total number of solutions $x \in \{1, \ldots, n\}$ of all congruences $x^2 \equiv 3 \pmod{n}$, where $\gcd(n, 6) = 1$ and $1 \leqslant n \leqslant N$. We will account for possible factors of 2 and 3 in n later; understanding the asymptotic behavior of $B_3(N)$ will be enough to understand $D_{2,3}(N)$.

Dirichlet characters

Definition 7

A *Dirichlet character of modulus m* (where m is a positive integer) is a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ which satisfies

1) $\chi(a)\chi(b) = \chi(ab)$,
2) $\chi(a + m) = \chi(a)$,
3) $\chi(a)$ is nonzero iff $\gcd(a, m) = 1$.

Dirichlet characters we use

1) $\chi_{8,1}, \chi_{8,3}$ and $\chi_{8,5}$, of modulus 8, as well as $\chi_{4,3}$ of modulus 4 defined by

	1	3	5	7
$\chi_{8,1}$	1	1	1	1
$\chi_{8,3}$	1	1	-1	-1
$\chi_{8,5}$	1	-1	-1	1
$\chi_{4,3}$	1	-1		

2) For any prime $q \equiv 1 \pmod 4$ we denote

$$\chi_{q,q-1}(a) = \left(\frac{q}{a}\right)$$

3) For any prime $q \equiv 3 \pmod 4$ we denote

$$\chi_{4q,4q-1}(a) = \left(\frac{4q}{a}\right),$$

Dirichlet L-functions

Definition 8

A *Dirichlet L-series* is a function of the form

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where χ is a Dirichlet character and s is a complex variable (with $\Re s > 1$). This function can be extended to a meromorphic function on the whole plane and is then called a *Dirichlet L-function*, also denoted by $L(s,\chi)$.

Dirichlet had shown that $L(s,\chi)$ is non-zero at $s = 1$. An L-function is entire whenever χ is not principal.

Dirichlet series

Euler (1737) proved the existence of infinitely many primes by showing that the series $\sum_{p\in\mathbb{P}} p^{-1}$ diverges. He deduced that $\zeta(s)$, given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for real $s > 1$, tends to ∞ as $s \to 1$.

Dirichlet series II

Dirichlet (1837) proved his theorem on primes in arithmetical progression by studying

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where χ is a Dirichlet character. Both $\zeta(s)$ and $L(s,\chi)$ are examples of *Dirichlet series*, i. e. they are of the form

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

where $f(n)$ is an arithmetical function.

Dirichlet series III

Some facts on them: if $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ does not converge for all s or does not diverge for all s, then there is a $\sigma_a \in \mathbb{R}$, *the abscissa of absolute convergence*, such that the series $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ converges absolutely if $\Re s > \sigma_a$, but does not converge absolutely if $\sigma < \sigma_a$.

Riemann's $\zeta(s)$ has $\sigma_a = 1$. L-series of Dirichlet characters have $\sigma_a \leqslant 1$.

Dirichlet series IV (from Apostol's book)

Theorem 11.5 *Given two functions $F(s)$ and $G(s)$ represented by Dirichlet series,*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \quad \text{for } \sigma > a,$$

and

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s} \quad \text{for } \sigma > b.$$

Then in the half-plane where both series converge absolutely we have

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}, \tag{5}$$

where $h = f * g$, the Dirichlet convolution of f and g:

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Conversely, if $F(s)G(s) = \sum \alpha(n)n^{-s}$ for all s in a sequence $\{s_k\}$ with $\sigma_k \to +\infty$ as $k \to \infty$ then $\alpha = f * g$.

Euler products

Theorem 9 ([2, Theorem 1.9])

If f is multiplicative and $\sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\sigma}} < \infty$, where σ is the real part of s, then the Dirichlet series of f has an Euler product, i. e.

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\right).$$

The weighted sum estimation

We define the following Dirichlet series:

$$\beta_q(s) := \mathcal{D}b_q(s) = \sum \frac{b_q(n)}{n^s}.$$

Lemma 10

Let $\mathcal{G}$ be a set of primes (called good primes). Let $\lambda_G \colon \mathbb{N} \to \{0, 1\}$ be the indicator function of a multiplicative monoid in $\mathbb{N}$ generated by $\mathcal{G}$. Then the Dirichlet series $\beta(s)$ of $b(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n)$ satisfies

$$\beta(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)},$$

for $\Re s > 1$, where $\zeta_{\mathcal{G}}(s)$ is

$$\zeta_{\mathcal{G}}(s) := \mathcal{D}\lambda_{\mathcal{G}}(s) = \sum_{n=1}^{\infty} \frac{\lambda_{\mathcal{G}}(n)}{n^s}.$$

Lemma proof I

We wish to express $b(n)$ as a convolution of two arithmetic functions. We need *the $\mathcal{G}$-modified Möbius function* which we define as

$$\mu_{\mathcal{G}}(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if n squarefree and } p \mid n \Rightarrow p \in \mathcal{G} \\ 0, & \text{otherwise} \end{cases} .$$

Lemma proof II

Now we can express

$$b(n) = 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) = \sum_{d|n} \mu_{\mathcal{G}}^2(d) \cdot \lambda_{\mathcal{G}}(n)$$

$$\stackrel{(**)}{=} \sum_{d|n} \mu_{\mathcal{G}}^2(d) \cdot \lambda_{\mathcal{G}}\left(\frac{n}{d}\right) = \left(\mu_{\mathcal{G}}^2 * \lambda_{\mathcal{G}}\right)(n)$$

Lemma proof III

Since $\mathcal{D}(\mu_{\mathcal{G}}^2 * \lambda_{\mathcal{G}})(s) = \mathcal{D}\mu_{\mathcal{G}}^2(s)\mathcal{D}\lambda_{\mathcal{G}}(s)$, we only need to calculate $\mathcal{D}\mu_{\mathcal{G}}^2(s)$. We can expand $\mathcal{D}\mu_{\mathcal{G}}^2(s)$ into an Euler product to obtain

$$\mathcal{D}(\mu_{\mathcal{G}}^2) = \prod_{p\in\mathcal{G}}\left(1+\frac{1}{p^s}\right) = \frac{\prod_{p\in\mathcal{G}}\left(1-\frac{1}{p^{2s}}\right)}{\prod_{p\in\mathcal{G}}\left(1-\frac{1}{p^s}\right)}$$

$$= \frac{\prod_{p\in\mathcal{G}}\left(1-\frac{1}{p^s}\right)^{-1}}{\prod_{p\in\mathcal{G}}\left(1-\frac{1}{p^{2s}}\right)^{-1}} = \frac{\zeta_{\mathcal{G}}(s)}{\zeta_{\mathcal{G}}(2s)}$$

$\square$

Recap

We have the set of good primes $\mathcal{G} = \mathcal{G}_3 = \{p \equiv \pm 1 \pmod{12}\}$.

We're estimating

$$B(N) = B_3(N) = \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) = \sum_{1 \leqslant n \leqslant N} b_3(n)$$

via its Dirichlet series $\beta(s)$ satisfying

$$\beta(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)},$$

where $\zeta_{\mathcal{G}}(s)$ is

$$\zeta_{\mathcal{G}}(s) := \mathcal{D}\lambda_{\mathcal{G}}(s) = \sum_{n=1}^{\infty} \frac{\lambda_{\mathcal{G}}(n)}{n^s}.$$

Estimation – next step

Rewrite $\zeta_{\mathcal{G}}(s)$:

$$\zeta_{\mathcal{G}}(s) = \prod_{p \in \mathcal{G}} (1 - p^{-s})^{-1} = \zeta(s) \prod_{p \notin \mathcal{G}} (1 - p^{-s})$$
$$= \zeta(s) \cdot (1 - 2^{-s})(1 - 3^{-s}) \cdot \prod_{p \equiv 5} (1 - p^{-s}) \prod_{p \equiv 7} (1 - p^{-s}).$$

Estimation – the ugliest slide

Plugging this in the expression for $\beta_q(s)$ we have

$$\frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1-2^{-s})^2(1-3^{-s})^2}{(1-2^{-2s})(1-3^{-2s})} \cdot \prod_{p\equiv 5} \frac{(1-p^{-s})^2}{(1-p^{-2s})} \prod_{p\equiv 7} \frac{(1-p^{-s})^2}{(1-p^{-2s})}$$
$$= \frac{\zeta^2(s)}{\zeta(2s)} \cdot \frac{(1-2^{-s})(1-3^{-s})}{(1+2^{-s})(1+3^{-s})} \cdot \prod_{p\equiv 5} \frac{(1-p^{-s})}{(1+p^{-s})} \cdot \prod_{p\equiv 7} \frac{(1-p^{-s})}{(1+p^{-s})}.$$

We further analyze the two last products by introducing other remainders modulo 12:

$$\prod_{p\equiv 1} \frac{(1-p^{-s})^{-1}}{(1-p^{-s})^{-1}} \cdot \prod_{p\equiv 5} \frac{(1+p^{-s})^{-1}}{(1-p^{-s})^{-1}} \prod_{p\equiv 7} \frac{(1+p^{-s})^{-1}}{(1-p^{-s})^{-1}} \cdot \prod_{p\equiv 11} \frac{(1-p^{-s})^{-1}}{(1-p^{-s})^{-1}}$$

Finally,

$$\beta(s) = \frac{\zeta^2(s)}{\zeta(2s)} \frac{(1-2^{-s})(1-3^{-s})}{(1+2^{-s})(1+3^{-s})} \cdot \frac{L(s,\chi_{12,11})}{L(s,\chi_{12,1})} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s,\chi_{12,11})}{(1+2^{-s})(1+3^{-s})}.$$

Lemma about our Dirichlet series

Lemma 11

The Dirichlet series of $b_3(n) = 2^{\omega(n)} \cdot \lambda_G(n)$ *satisfies*

$$\beta_3(s) = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{12,11})}{(1+2^{-s})(1+3^{-s})}.$$

For general prime $q \equiv 3 \pmod 4$,

$$\beta_q(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{4|q|,4|q|-1})}{(1+2^{-s})(1+|q|^{-s})}.$$

Tauberian theorem

Theorem 12 (Corollary of Wiener-Ikehara [3])

Let $a(n) \geqslant 0$. *If the Dirichlet series of the form*

$$\sum_{n=1}^{\infty} a(n) n^{-s}$$

converges to an analytic function in the half-plane $\Re(s) > 1$ *with a simple pole of residue* c *at* $s = 1$, *then*

$$\sum_{n \leqslant N} a(n) \sim cN.$$

Application of Wiener-Ikehara

$$\beta_3(s) = \frac{\zeta_{\mathcal{G}}^2(s)}{\zeta_{\mathcal{G}}(2s)} = \frac{\zeta(s)}{\zeta(2s)} \cdot \frac{L(s, \chi_{12,11})}{(1+2^{-s})(1+3^{-s})}$$

is analytic on the half-plane for $\Re(s) > 1$, so we need its residue at $s = 1$.
Only $\zeta(s)$ is not holomorphic at $s = 1$ & denominators have no zeroes for $\Re(s) > \frac{1}{2}$. The residue of $\beta_3(s)$ at $s = 1$ is

$$\frac{L(1, \chi_{12,11})}{\zeta(2) \cdot 3/2 \cdot 4/3} = \frac{L(1, \chi_{12,11})}{2\zeta(2)}.$$

Hence $B(N) \sim \frac{L(1,\chi_{12,11})}{2\zeta(2)} N$.

Accounting for factors of 2 and $q = 3$

$$B(N) \sim \frac{L(1, \chi_{12,11})}{2\zeta(2)} N.$$

Theorem 13

Let prime $q \equiv 3 \pmod{4}$. Then $D_{2,q}(N)$, the number of $D(q)$-pairs up to N, satisfies

$$D_{2,q}(N) \sim \left(1 + \frac{1}{2} + \frac{1}{q} + \frac{1}{2q}\right) B(N) = \frac{L(1, \chi_{4|q|,4|q|-1})}{\zeta(2)} N.$$

One slide about the final part for $q \equiv 3 \pmod 4$

$$
\begin{aligned}
D_{2,q}(N) = & \sum_{1 \leqslant n \leqslant N} 2^{\omega(n)} \cdot \lambda_{\mathcal{G}}(n) + \sum_{\substack{1 \leqslant n \leqslant N \\ 2 || n}} 2^{\omega(n)-1} \cdot \lambda_{\mathcal{G}}\left(\frac{n}{2}\right) + \\
& + \sum_{\substack{1 \leqslant n \leqslant N \\ q || n}} 2^{\omega(n)-1} \cdot \lambda_{\mathcal{G}}\left(\frac{n}{q}\right) + \sum_{\substack{1 \leqslant n \leqslant N \\ 2,q || n}} 2^{\omega(n)-2} \cdot \lambda_{\mathcal{G}}\left(\frac{n}{2q}\right) \\
= & B(N) + B\left(\left\lfloor \frac{N}{2} \right\rfloor\right) + B\left(\left\lfloor \frac{N}{q} \right\rfloor\right) + B\left(\left\lfloor \frac{N}{2q} \right\rfloor\right) \\
= & \left(1 + \frac{1}{2} + \frac{1}{q} + \frac{1}{2q}\right) B(N) + O(1).
\end{aligned}
$$

Counting $D(n)$-triples

Definition 14

Let $a < b < c$. A $D(n)$-triple $\{a, b, c\}$ is called *regular* if $c = a + b + 2r$, where $r^2 = ab + n$. A $D(n)$-triple $\{a, b, c\}$ is called *irregular* if it is not regular.

Let $D_{3,n}^{\text{reg}}(N)$ denote the number of regular $D(n)$-triples $\{a, b, c\}$ such that $a < b < c \leqslant N$.

The following theorem holds for all integers n, and its proof is mostly concerned with showing that different cases give at most $O(1)$-triples.

Counting $D(n)$-triples II

Theorem 15 (Minor refinement of Theorem 3)

Let n be an integer. The number of $D(n)$-triples with all elements in the set $\{1, 2, \ldots, N\}$ is asymptotically equal to the number of regular $D(n)$-triples, which is in turn half the number of $D(n)$-pairs. More precisely,

$$D_{3,n}(N) \sim D_{3,n}^{reg}(N) \sim \frac{D_{2,n}(N)}{2}.$$

Proof of the theorem

Since $\{a, b, c\}$ is a $D(n)$-triple, there exist positive integers r, s, t satisfying $ab + n = r^2, ac + n = s^2, bc + n = t^2$. According to [1, Lemma 3][1], there exist integers e, x, y, z such that

$$ae + n^2 = x^2, be + n^2 = y^2, ce + n^2 = z^2,$$

and

$$c = a + b + \frac{e}{n} + \frac{2}{n^2}(abe + rxy), \tag{1}$$

We consider three cases, depending on the sign of e.

[1] A. Dujella, "On the size of Diophantine m-tuples", Math. Proc. Cambridge Philos. Soc. 132, no. 1 (2002): 23–33.

Proof of the theorem II

1) If $e < 0$, then $c \leqslant n^2$. Hence, the number of such triples is $O(1)$ (it is less then $\frac{n^6}{6}$, so the implied constant in O depends on n).

2) If $e = 0$, then $c = a + b + 2r$. Also, $b = a + c - 2s$, where $ac + n = s^2$, $s \geqslant 0$. Every pair $\{a, c\}, ac + n = s^2, a < c \leqslant N$ induces a regular $D(n)$ triple $\{a, a + c - 2s, c\} \subseteq \{1, 2, \ldots, N\}$, unless $a + c - 2s > N$, $a + c - 2s \leqslant 0$, or $a + c - 2s = a$, or $a + c - 2s = c$. The inequality $a + c - 2s > N$ implies $a - 2s > N - c \geqslant 0$. However, $a > 2s$ implies $a^2 > 4s^2 = 4ac + 4n$, i. e. $-4n > a(4c - a) > a \cdot 3c$, which can hold only if $c < \frac{4}{3}|n|$. Therefore the contribution of this case is $O(n) = O(1)$. Similar arguments hold for other degenerate cases (in one of them, one gets $(c - a)^2 = 4n$).

Proof of the theorem III

2) cont'd Every regular $D(n)$-triple $\{a, b, c\}$ is obtained twice by this construction: from $\{a, c\}$ and from $\{b, c\}$. Thus, the total contribution of the case 2), i. e. the number of regular $D(n)$-triples, is

$$D_{3,n} = \frac{1}{2}\left(D_{2,n}(N) - N \cdot [n \text{ is a square}] + O(1)\right).$$

3) If $e \geqslant 1$, then

$$c = a+b+\frac{e}{n}+\frac{2abe}{n^2}+\frac{2\sqrt{(ab+n)\left(ae+n^2\right)\left(be+n^2\right)}}{n^2} > \frac{2ab}{n^2}.$$

For now, let us assume that $ab > n$. We have $N \geqslant c \geqslant \frac{2ab}{n^2} > \frac{r^2}{n^2}$.

Let us estimate the number of such pairs $\{a, b\}$ satisfying

$$ab + n = r^2, \quad r < n\sqrt{N}.$$

Proof of the theorem IV – 3) cont'd

Consider the congruence $x^2 \equiv n \pmod{a}$. In each interval of size a, there are at most $2^{\omega(a)+1}$ solutions. Hence, the number of pairs $\{a, b\}$ is bounded above by

$$\sum_{a=1}^{n\sqrt{N}} 2^{\omega(a)+1} \cdot \left(\frac{n\sqrt{N}}{a} + 1\right) = 2n\sqrt{N} \sum_{a=1}^{n\sqrt{N}} \frac{2^{\omega(a)}}{a} + 2 \sum_{a=1}^{n\sqrt{N}} 2^{\omega(a)}$$
$$= O\left(\sqrt{N} \log^2 N\right) + O(\sqrt{N} \log N)$$
$$= O\left(\sqrt{N} \log^2 N\right)$$

On the other hand, if $ab \leqslant n$, adding at most $O(n^2)$-pairs $\{a, b\}$ to the above estimate does not change it.

If a and b are given, then finding c is equivalent to choosing a solution of the Pellian equation

$$bs^2 - at^2 = n(b-a).$$

In each sequence there are $O(\log N)$ solutions with $s \leqslant N$. The number of the sequences is bounded by $2^{k+\omega(n)+1}$, where $k = \omega(b-a)$. We have $b - a \geqslant p_1 \cdots p_k$ and $\log b > \log(b-a) > \frac{1}{2}p_k > \frac{1}{2}k \log k$. We get

$$k < \frac{2\log b}{\log k}.$$

Proof of the theorem VI – 3) finished

Therefore, we can conclude that

$$2^k < 2^{\frac{2\log b}{\log k}} < b^{\frac{1.4}{\log k}}.$$

If $2^k \geqslant b^{0.01}$, then we have $k < e^{140}$ and $b < 2^{100\cdot e^{140}}$, hence, the number of such sequences is $O(1)$. If $2^k < b^{0.01}$, then the number of the corresponding sequences is less that $2\cdot 2^{\omega(n)}\cdot N^{0.01}$. Therefore, the contribution of the case 3) is

$$O\left(\sqrt{N}\log^2 N\cdot N^{0.01}\cdot\log N\right) = O\left(N^{0.52}\right).$$

Byproduct of our proof

Corollary 16

If an irregular $D(n)$-triple $\{a, b, c\}$ satisfies $a < b < c$ and $c > n^2$, then

$$c \geqslant \frac{2}{n^2} ab.$$

For positive n, this lower bound can be improved to $c \geqslant \frac{4}{n^2} ab$.

The number of $D(q)$-triples for prime q

Corollary 17

Let q be an integer such that $|q|$ is a prime or $q = -1$. The number of $D(q)$-triples is given by the following.

a) *For even q,*

$$D_{3,2}(N) \sim \frac{L(1, \chi_{8,5})}{2\zeta(2)} \cdot N, \quad \textit{while } D_{3,-2}(N) \sim \frac{L(1, \chi_{8,3})}{2\zeta(2)} \cdot N.$$

b) *Let $q \equiv 3 \pmod 4$ such that $|q|$ is prime, or $q = -1$. Then*

$$D_{3,q}(N) \sim \frac{L(1, \chi_{4|q|,4|q|-1})}{2\zeta(2)} \cdot N.$$

The number of $D(q)$-triples for prime q II

c) Let $q \equiv 5 \pmod 8$ such that $|q|$ is prime. Then

$$D_{3,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{\zeta(2)} \cdot N.$$

d) Let $q \equiv 1 \pmod 8$ such that $|q|$ is prime. Then

$$D_{3,q}(N) \sim \frac{L(1, \chi_{|q|,|q|-1})}{2\zeta(2)} \cdot N.$$

Further work

- the number of $D(n)$-pairs for composite n-s
- estimating the error terms?
- finding infinitely many $D(n)$-quadruples for non-square ns???