Addition sequences and numerical evaluation of modular forms

Fredrik Johansson (INRIA Bordeaux)

Joint work with
Andreas Enge (INRIA Bordeaux)
William Hart (TU Kaiserslautern)

DK Statusseminar in Strobl, September 30, 2015

Modular forms

A **modular form** of weight k is a holomorphic function on $\mathbb{H} = \{\tau : \tau \in \mathbb{C}, \mathrm{im}(\tau) > 0\}$ satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)$$

for any integers a, b, c, d with $ad - bc = 1$. A **modular function** is meromorphic and has weight $k = 0$.

Modular forms

A **modular form** of weight k is a holomorphic function on $\mathbb{H} = \{\tau : \tau \in \mathbb{C}, \mathrm{im}(\tau) > 0\}$ satisfying

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau)$$

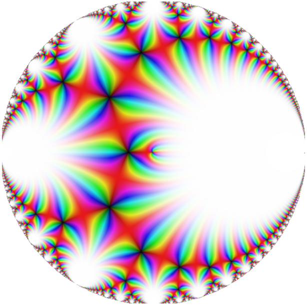
for any integers a, b, c, d with $ad - bc = 1$. A **modular function** is meromorphic and has weight $k = 0$.

Since $f(\tau) = f(\tau + 1)$, it has a Fourier series (q-expansion)

$$f(\tau) = \sum_{n=-m}^{\infty} c_n e^{2i\pi n\tau} = \sum_{n=-m}^{\infty} c_n q^n$$

where $q = e^{2\pi i\tau}$ (note that $|q| < 1$).

Picture of a modular function: the j-function $j(\tau)$

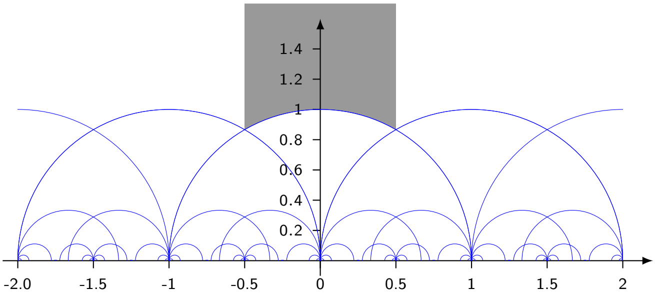


As a function of $\tau \in [-2,2] + [0,1]i$ (top) and of q (bottom).

Numerical evaluation

By repeated use of $\tau \to \tau + 1$ or $\tau \to -1/\tau$, we can move τ to the *fundamental domain* $\left\{\tau \in \mathbb{H} : |z| \geq 1, |\mathrm{Re}(z)| \leq \frac{1}{2}\right\}$.

In the fundamental domain, $|q| \leq \exp(-\pi\sqrt{3}) = 0.00433\ldots$, which gives rapid convergence of the q-expansion.



[Source for illustration: user "Tom Bombadil" on TeX StackExchange.]

Example: the j-function

Any elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{C}$ can be identified with a complex lattice $(1, \tau)$.

Example: the j-function

Any elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{C}$ can be identified with a complex lattice $(1, \tau)$.

The j-function describes isomorphism classes of elliptic curves.
It is a modular function ($j(\tau) = j(\tau + 1) = j(-1/\tau)$) and has the q-expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

Example: the j-function

Any elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{C}$ can be identified with a complex lattice $(1, \tau)$.

The j-function describes isomorphism classes of elliptic curves.
It is a modular function ($j(\tau) = j(\tau + 1) = j(-1/\tau)$) and has the q-expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

The j-function has magical properties:

- At certain algebraic τ, the value $j(\tau)$ is also algebraic
- $e^{\pi\sqrt{163}} = 640320^3 + 743.99999999999925007\ldots$
- The q-expansion is related to the "monster group"
- ...

The Hilbert class polynomial

For $D < 0$ congruent to 0 or 1 mod 4,

$$H_D(x) = \prod_{(a,b,c)} \left(x - j\left(\frac{-b + \sqrt{D}}{2a} \right) \right) \in \mathbb{Z}[x]$$

where (a, b, c) is taken over all the primitive reduced binary quadratic forms $ax^2 + bxy + cy^2$ with $b^2 - 4ac = D$.

The Hilbert class polynomial

For $D < 0$ congruent to 0 or 1 mod 4,

$$H_D(x) = \prod_{(a,b,c)} \left(x - j\left(\frac{-b+\sqrt{D}}{2a} \right) \right) \in \mathbb{Z}[x]$$

where (a, b, c) is taken over all the primitive reduced binary quadratic forms $ax^2 + bxy + cy^2$ with $b^2 - 4ac = D$.

Application: constructing elliptic curves with a prescribed number of points over a finite field (useful in primality proving, cryptography).

The first few Hilbert class polynomials

D	H_D
-3	x
-4	$x - 1728$
-7	$x + 3375$
-8	$x - 8000$
-11	$x + 32768$
-12	$x - 54000$
-15	$x^2 + 191025x - 121287375$
-16	$x - 287496$
-19	$x + 884736$
-20	$x^2 - 1264000x - 681472000$
-23	$x^3 + 3491750x^2 - 5151296875x + 12771880859375$
-24	$x^2 - 4834944x + 14670139392$
-27	$x + 12288000$
-28	$x - 16581375$
-31	$x^3 + 39491307x^2 - 58682638134x + 1566028350940383$

Numerical example

The quadratic forms with discriminant $D = -31$ are

$$x^2 + xy + 8y^2, \quad 2x^2 + xy + 4y^2, \quad 2x^2 - xy + 4y^2$$

Numerical example

The quadratic forms with discriminant $D = -31$ are

$$x^2 + xy + 8y^2, \quad 2x^2 + xy + 4y^2, \quad 2x^2 - xy + 4y^2$$

Therefore $H_{-31} = (x - j_1)(x - j_2)(x - j_3)$ where

$$j_1 = j\left(\tfrac{-1+\sqrt{-31}}{2}\right), \quad j_2 = j\left(\tfrac{-1+\sqrt{-31}}{4}\right), \quad j_3 = \bar{j_2} = j\left(\tfrac{+1+\sqrt{-31}}{4}\right)$$

Numerical example

The quadratic forms with discriminant $D = -31$ are

$$x^2 + xy + 8y^2, \quad 2x^2 + xy + 4y^2, \quad 2x^2 - xy + 4y^2$$

Therefore $H_{-31} = (x - j_1)(x - j_2)(x - j_3)$ where

$$j_1 = j\left(\tfrac{-1+\sqrt{-31}}{2}\right), \quad j_2 = j\left(\tfrac{-1+\sqrt{-31}}{4}\right), \quad j_3 = \bar{j_2} = j\left(\tfrac{+1+\sqrt{-31}}{4}\right)$$

Using ball arithmetic with 73 bits of precision, we compute

$$\begin{aligned} j_1 &= [-39492793.91155624414 \pm 6.10 \cdot 10^{-12}] \\ j_2 &= [743.455778122071940 \pm 3.22 \cdot 10^{-16}] \\ &\quad + [6253.062846903285089 \pm 8.87 \cdot 10^{-16}]i \end{aligned}$$

Numerical example

The quadratic forms with discriminant $D = -31$ are

$$x^2 + xy + 8y^2, \quad 2x^2 + xy + 4y^2, \quad 2x^2 - xy + 4y^2$$

Therefore $H_{-31} = (x - j_1)(x - j_2)(x - j_3)$ where

$$j_1 = j\left(\tfrac{-1+\sqrt{-31}}{2}\right), \quad j_2 = j\left(\tfrac{-1+\sqrt{-31}}{4}\right), \quad j_3 = \bar{j_2} = j\left(\tfrac{+1+\sqrt{-31}}{4}\right)$$

Using ball arithmetic with 73 bits of precision, we compute

$$\begin{aligned} j_1 &= [-39492793.91155624414 \pm 6.10 \cdot 10^{-12}] \\ j_2 &= [743.455778122071940 \pm 3.22 \cdot 10^{-16}] \\ &\quad + [6253.062846903285089 \pm 8.87 \cdot 10^{-16}]i \end{aligned}$$

Expanding gives $H_{-31} = x^3 + c_2x^2 + c_1x + c_0$ where

$$\begin{aligned} c_2 &= [39491307.00000000000 \pm 2.44 \cdot 10^{-12}] \\ c_1 &= [-58682638134.0000000 \pm 1.61 \cdot 10^{-8}] \\ c_0 &= [1566028350940383.000 \pm 3.22 \cdot 10^{-4}] \end{aligned}$$

Computing H_D

Problem: for large D, H_D is huge!

- $\deg(H_D) = O(|D|^{1/2+\varepsilon})$
- $\max \log_2 |[x^k]H_D| = O(|D|^{1/2+\varepsilon})$
- Total size of H_D: $O(|D|^{1+\varepsilon})$ bits

Several competing methods (complex analytic, p-adic, and Chinese remaindering methods) each allow computing H_D with complexity $O(|D|^{1+\varepsilon})$.

Computing H_D

Problem: for large D, H_D is huge!

- $\deg(H_D) = O(|D|^{1/2+\varepsilon})$
- $\max \log_2 |[x^k]H_D| = O(|D|^{1/2+\varepsilon})$
- Total size of H_D: $O(|D|^{1+\varepsilon})$ bits

Several competing methods (complex analytic, p-adic, and Chinese remaindering methods) each allow computing H_D with complexity $O(|D|^{1+\varepsilon})$.

Enge (2009): complexity analysis and tight coefficient bounds for the complex analytic method. Depends on asymptotically fast polynomial arithmetic over $\mathbb{R}$. Without complete proofs for floating-point rounding errors.

New: a fast, rigorous implementation

Sage: complex analytic (floating-point)

Pari/GP: CRT method, by Hamish Ivey-Law

CM: complex analytic (floating-point), by Andreas Enge

Arb: complex analytic (ball arithmetic), by FJ

D	deg	bits	Sage	Pari/GP	CM	Arb
$-1\,000\,003$	105	8527	2.1 s	12 s	0.7 s	0.33 s
$-10\,000\,003$	706	50889	601 s	290 s	101 s	46 s
$-100\,000\,003$	1702	153095			1822 s	750 s

The expensive steps when computing H_D

A. Compute numerical approximations of the $j(\tau)$ values

B. Multiply together the linear factors $(x - j(\tau))$

In practice, the bottleneck is A.

This leads to the question of how much this task (and more generally, numerical evaluation of other modular forms/functions) can be optimized.

Choice of q-expansion

Recall

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

The coefficients grow like

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}$$

Choice of q-expansion

Recall

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

The coefficients grow like

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}$$

In practice, one rewrites the modular form/function one wishes to compute in terms of either:

- The Dedekind eta function
- Jacobi theta functions

These functions not only have small and explicit coefficients ($c_n = \pm 1$), but their q-expansions are *sparse*.

The Dedekind eta function

$$\begin{aligned}\eta(\tau) &= e^{\pi i\tau/12}\prod_{k=1}^{\infty}(1-q^k) = e^{\pi i\tau/12}\sum_{k=-\infty}^{\infty}(-1)^k q^{(3k^2-k)/2}\\ &= e^{\pi i\tau/12}\left(1-q-q^2+q^5+q^7-q^{12}-q^{15}+\dots\right)\end{aligned}$$

The Dedekind eta function

$$\eta(\tau) = e^{\pi i \tau/12} \prod_{k=1}^{\infty} (1 - q^k) = e^{\pi i \tau/12} \sum_{k=-\infty}^{\infty} (-1)^k q^{(3k^2-k)/2}$$
$$= e^{\pi i \tau/12} \left(1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \ldots\right)$$

The exponents $P(k) = (3k^2 - k)/2$ are the *pentagonal numbers*.

$$P(0), P(1), P(2), \ldots = 0, 1, 5, 12, 22, \ldots$$

$$P(-1), P(-2), \ldots = 2, 7, 15, 26, \ldots$$

For d digits, we only need $O(d^{1/2})$ terms of the q-expansion!

The Dedekind eta function

$$\eta(\tau) = e^{\pi i \tau/12} \prod_{k=1}^{\infty} (1 - q^k) = e^{\pi i \tau/12} \sum_{k=-\infty}^{\infty} (-1)^k q^{(3k^2-k)/2}$$
$$= e^{\pi i \tau/12} \left(1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \ldots\right)$$

The exponents $P(k) = (3k^2 - k)/2$ are the *pentagonal numbers*.

$$P(0), P(1), P(2), \ldots = 0, 1, 5, 12, 22, \ldots$$

$$P(-1), P(-2), \ldots = 2, 7, 15, 26, \ldots$$

For d digits, we only need $O(d^{1/2})$ terms of the q-expansion!

$$j(\tau) = \left(\left(\frac{\eta(\tau)}{\eta(2\tau)} \right)^8 + 2^8 \left(\frac{\eta(2\tau)}{\eta(\tau)} \right)^{16} \right)^3$$

Properties of the eta function

It is a modular form of weight $1/2$:

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right)=\varepsilon(a,b,c,d)(c\tau+d)^{1/2}\eta(\tau)$$

where $\varepsilon(a,b,c,d)$ is a certain 24th root of unity.

Properties of the eta function

It is a modular form of weight $1/2$:

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \varepsilon(a,b,c,d)(c\tau+d)^{1/2}\eta(\tau)$$

where $\varepsilon(a,b,c,d)$ is a certain 24th root of unity.

It generates the partition function $p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$:

$$e^{\pi i\tau/12}/\eta(\tau) = \sum_{n=0}^{\infty} p(n)q^n = 1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + \dots$$

Properties of the eta function

It is a modular form of weight $1/2$:

$$\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \varepsilon(a,b,c,d)(c\tau+d)^{1/2}\eta(\tau)$$

where $\varepsilon(a,b,c,d)$ is a certain 24th root of unity.

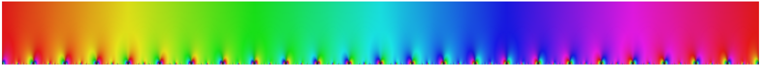
It generates the partition function $p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$:

$$e^{\pi i\tau/12}/\eta(\tau) = \sum_{n=0}^{\infty} p(n)q^n = 1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + \ldots$$

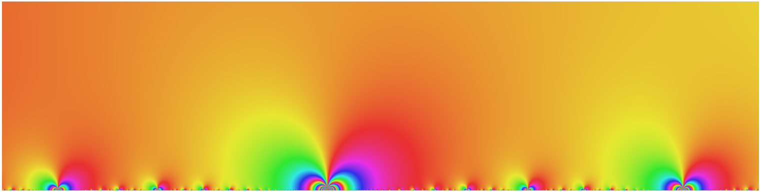
It has interesting special values such as

$$\eta(i) = \frac{\Gamma\left(1/4\right)}{2\pi^{3/4}}$$

Pictures of $\eta(\tau)$



Overview: $\tau \in [0, 24] + [0, 1]i$



Deep zoom: $\tau \in [\sqrt{2}, \sqrt{2} + 10^{-101}] + [0, 2.5 \times 10^{-102}]i$

Computing the Dedekind eta function

$$\eta(\tau) = e^{\pi i \tau / 12} \left(1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \ldots\right)$$

We compute $\eta(i)$ to 50-digit precision.

$+q^0$	$+1.0000000000000000000000000000000000000000000000000$
$-q^1$	$-0.0018674427317079888144302129348270303934228050024\ldots$
$-q^2$	$-0.0000034873423562089954917752662652081277882033550\ldots$
$+q^5$	$+0.0000000000000227110106832409383867927523909354754\ldots$
$+q^7$	$+0.0000000000000000000792010695079811226359059422276\ldots$
$-q^{12}$	$-0.0000000000000000000000000000000017987363357198674\ldots$
$-q^{15}$	$-0.0000000000000000000000000000000000000000117141123\ldots$

$$\eta(i) = 0.76822542232605665900259417957618064451786691446480\ldots$$

Jacobi theta functions

$$\theta_1(z,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i[(n+\frac{1}{2})^2\tau+(2n+1)z+n-\frac{1}{2}]} = 2q' \sum_{n=0}^{\infty}(-1)^n q^{n(n+1)} \sin((2n+1)\pi z)$$

$$\theta_2(z,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i[(n+\frac{1}{2})^2\tau+(2n+1)z]} = 2q' \sum_{n=0}^{\infty} q^{n(n+1)} \cos((2n+1)\pi z)$$

$$\theta_3(z,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i[n^2\tau+2nz]} = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \cos(2n\pi z)$$

$$\theta_4(z,\tau) = \sum_{n=-\infty}^{\infty} e^{\pi i[n^2\tau+2nz+n]} = 1 + 2\sum_{n=1}^{\infty}(-1)^n q^{n^2} \cos(2n\pi z)$$

$$q = \exp(\pi i\tau), \qquad q' = \exp(\pi i\tau/4)$$

We only require the "theta constants" which have $z = 0$.

Theta constants

$$\theta_2(\tau) = 2q' \sum_{n=0}^{\infty} q^{n(n+1)} = 2q'(1 + q^2 + q^6 + q^{12} + q^{20} + \dots)$$

$$\theta_3(\tau) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \dots$$

$$\theta_4(\tau) = 1 + 2\sum_{n=1}^{\infty} (-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + 2q^{16} - \dots$$

The exponents $n(n+1)$ are the *trigonal numbers*
The exponents n^2 are the *square numbers*

Theta constants

$$\theta_2(\tau) = 2q' \sum_{n=0}^{\infty} q^{n(n+1)} = 2q'(1 + q^2 + q^6 + q^{12} + q^{20} + \dots)$$

$$\theta_3(\tau) = 1 + 2 \sum_{n=1}^{\infty} q^{n^2} = 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \dots$$

$$\theta_4(\tau) = 1 + 2 \sum_{n=1}^{\infty} (-1)^n q^{n^2} = 1 - 2q + 2q^4 - 2q^9 + 2q^{16} - \dots$$

The exponents $n(n+1)$ are the *trigonal numbers*
The exponents n^2 are the *square numbers*

$$j(\tau) = 32 \frac{(\theta_2(\tau)^8 + \theta_3(\tau)^8 + \theta_4(\tau)^8)^3}{(\theta_2(\tau)\theta_3(\tau)\theta_4(\tau))^8}$$

$$2\eta(\tau)^3 = \theta_2(\tau)\theta_3(\tau)\theta_4(\tau)$$

Addition sequences

We call a sequence of increasing positive integers $c_0, c_1, \dots$ an *addition sequence* if for every $c_k \neq 1$, there exist $i, j < k$ such that

$$c_k = c_i + c_j.$$

More formally, an addition sequence specifies the triples (c_k, c_i, c_j).

Addition sequences

We call a sequence of increasing positive integers $c_0, c_1, \ldots$ an *addition sequence* if for every $c_k \neq 1$, there exist $i, j < k$ such that

$$c_k = c_i + c_j.$$

More formally, an addition sequence specifies the triples (c_k, c_i, c_j).

An addition sequence of length n for a finite list of exponents $c_0, c_1, \ldots, c_n$ gives us an algorithm to compute the powers

$$q^{c_0}, q^{c_1}, q^{c_2}, \ldots, q^{c_n}$$

using n multiplications

$$q^{c_k} = q^{c_i} \cdot q^{c_j}.$$

Examples

Some sequences are already addition sequences:

$$n = 1, 2, 3, 4, 5, 6, \ldots$$

$$10n = (1, 2, 4, 5), 10, 20, 30, 40, 50, \ldots$$

$$F_n = 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

$$2^n = 1, 2, 4, 8, 16, 32, 64, 128, 256, \ldots$$

Others are not, and have to be extended:

$$n(n+1) = 2, 6, 12, 20, 30, 42, \ldots$$

$$n^2 : 1, 4, 9, 16, 25, 36, 49, 64, \ldots$$

$$3n(n-1)/2 = 1, 2, 5, 7, 12, 15, 22, 26, \ldots$$

$$3^n = 1, 3, 9, 27, 81, 243, 729, 2187, \ldots$$

Side note

Downey, Leong, Sethi (1981): the associated decision problem

> *Given $c_0, \ldots, c_n$ and a bound N, is there an addition sequence for $c_0, \ldots, c_n$ of length $\leq N$?*

is NP-complete.

A general way to construct addition sequences

Given a set of positive integers $C = \{c_0, \ldots, c_n\}$ with $c_0 < c_1 < \ldots < c_n$, it is clearly possible to construct an addition sequence for C having length

$$O(n \log c_n).$$

A general way to construct addition sequences

Given a set of positive integers $C = \{c_0, \ldots, c_n\}$ with $c_0 < c_1 < \ldots < c_n$, it is clearly possible to construct an addition sequence for C having length

$$O(n \log c_n).$$

Algorithm: if some element $c_i \in C$, $c_i \neq 1$, is not a sum of two smaller elements, adjoin $\lfloor c_i/2 \rfloor$ and $c_i - \lfloor c_i/2 \rfloor$ and start over.

A general way to construct addition sequences

Given a set of positive integers $C = \{c_0, \ldots, c_n\}$ with $c_0 < c_1 < \ldots < c_n$, it is clearly possible to construct an addition sequence for C having length

$$O(n \log c_n).$$

Algorithm: if some element $c_i \in C$, $c_i \neq 1$, is not a sum of two smaller elements, adjoin $\lfloor c_i/2 \rfloor$ and $c_i - \lfloor c_i/2 \rfloor$ and start over.

A more elaborate method gives (Yao 1976, cited in Knuth 4.6.3 exercise 37)

$$O\left(\log c_n + n \frac{\log c_n}{\log \log c_n} + \frac{\log c_n \log \log \log c_n}{(\log \log c_n)^2}\right)$$

Shorter addition sequences for polynomials

For any integer-valued polynomial $f \in \mathbb{Q}[X]$ of degree D, the consecutive values $f(1), f(2), \ldots, f(n)$ can be computed using $Dn + O(1)$ additions.

Use the system of recurrences given by iterated differences:

$$\begin{aligned} f(X) = f_D(X) &= f_D(X-1) + f_{D-1}(X-1) \\ f_{D-1}(X) &= f_{D-1}(X-1) + f_{D-2}(X-1) \\ \vdots &= \vdots \\ f_1(X) &= f_1(X-1) + f_0(X-1) \\ f_0(X) &= \text{constant} \end{aligned}$$

For $D = 2$ (including trigonal, square, pentagonal numbers), this method gives an addition sequence of length $2n + O(1)$.

Even shorter addition sequences for polynomials

Dobkin, Lipton (1980):

1. The n first squares $c_n = n^2$ can be computed using

$$n + O(n/\sqrt{\log n}) = n + o(n)$$

additions.

Even shorter addition sequences for polynomials

Dobkin, Lipton (1980):

1. The n first squares $c_n = n^2$ can be computed using

$$n + O(n/\sqrt{\log n}) = n + o(n)$$

additions.

2. For the squares, cubes, ..., and more generally k-th powers $c_n = n^k$, evaluating the first n terms requires at least $n + n^{2/3-\varepsilon}$ additions. This result also holds for a larger class of polynomials.

New results (EHJ)

For trigonal, square and pentagonal numbers:

1. Theorems regarding addition sequences of special form. The special addition sequences allow computing $\sum_{k=0}^{n} q^{c_k}$ using $n + o(n)$ multiplications (heuristically).

2. Computing $\sum_{k=0}^{n} q^{c_k}$ using $o(n)$ multiplications.

Pentagonal numbers

Theorem $c = 2a + b$**:** Every pentagonal number $c \geq 2$ is the sum of a smaller one and twice a smaller one, that is, there are pentagonal numbers $a, b < c$ such that $c = 2a + b$.

$\Rightarrow q^c = (q^a)^2 \cdot q^b$ always works

Pentagonal numbers

Theorem $c = 2a + b$**:** Every pentagonal number $c \geq 2$ is the sum of a smaller one and twice a smaller one, that is, there are pentagonal numbers $a, b < c$ such that $c = 2a + b$.

$\Rightarrow q^c = (q^a)^2 \cdot q^b$ always works

Theorem $c = a + b$**:** A pentagonal number $c \geq 2$ is the sum of two smaller ones, that is, there are pentagonal numbers $a, b < c$ such that $c = a + b$, if and only if $12c + 1$ is not a prime.

$\Rightarrow q^c = q^a \cdot q^b$ almost always works (heuristically)

Pentagonal numbers

Theorem $c = 2a + b$: Every pentagonal number $c \geq 2$ is the sum of a smaller one and twice a smaller one, that is, there are pentagonal numbers $a, b < c$ such that $c = 2a + b$.

$\Rightarrow q^c = (q^a)^2 \cdot q^b$ always works

Theorem $c = a + b$: A pentagonal number $c \geq 2$ is the sum of two smaller ones, that is, there are pentagonal numbers $a, b < c$ such that $c = a + b$, if and only if $12c + 1$ is not a prime.

$\Rightarrow q^c = q^a \cdot q^b$ almost always works (heuristically)

Conjecture: the first n pentagonal numbers can be computed using $n + O(n/\log n)$ additions

Pentagonal numbers

c	$a+b$	$2a+b$
2	$(1,1)$	$(1,0)$
5		$(2,1)$
7	$(2,5)$	$(1,5)$
12	$(5,7)$	$(5,2)$
15		$(5,5)$ $(7,1)$
22	$(7,15)$	$(5,12)$
26		$(2,22)$ $(7,12)$ $(12,2)$
35		$(15,5)$
40	$(5,35)$	$(7,26)$
51		$(22,7)$
57	$(22,35)$	$(26,5)$
70	$(35,35)$	$(15,40)$ $(22,26)$ $(35,0)$
77	$(7,70)$ $(26,51)$	$(35,7)$
92	$(15,77)$ $(22,70)$ $(35,57)$	$(26,40)$ $(35,22)$ $(40,12)$
100		$(15,70)$

Squares and trigonal numbers

We want to compute $\theta_2(\tau)$, $\theta_3(\tau)$ and $\theta_4(\tau)$ simultaneously.

The *quarter-squares* $t(n) = \lfloor (n+1)^2/4 \rfloor$ consist of the squares $t(2m-1) = m^2$ and trigonal numbers $t(2m) = m(m+1)$ interleaved in increasing order.

Squares and trigonal numbers

We want to compute $\theta_2(\tau)$, $\theta_3(\tau)$ and $\theta_4(\tau)$ simultaneously.

The *quarter-squares* $t(n) = \lfloor (n+1)^2/4 \rfloor$ consist of the squares $t(2m-1) = m^2$ and trigonal numbers $t(2m) = m(m+1)$ interleaved in increasing order.

Theorem $c = 2a + b$**:** Every quarter-square $c \geq 2$ is the sum of a smaller one and twice a smaller one, that is, there are quarter-squares $a, b < c$ such that $c = 2a + b$.

$\Rightarrow q^c = (q^a)^2 \cdot q^b$ always works

Quarter-squares

c	$a+b$	$2a+b$
2	$(1,1)$	$(1,0)$
4	$(2,2)$	$(1,2)$ $(2,0)$
6	$(2,4)$	$(1,4)$ $(2,2)$
9		$(4,1)$
12	$(6,6)$	$(4,4)$ $(6,0)$
16	$(4,12)$	$(2,12)$ $(6,4)$
20	$(4,16)$	$(2,16)$ $(4,12)$ $(9,2)$
25	$(9,16)$	$(12,1)$
30		$(9,12)$ $(12,6)$
36	$(6,30)$ $(16,20)$	$(12,12)$ $(16,4)$
42	$(6,36)$ $(12,30)$	$(6,30)$ $(20,2)$
49		$(12,25)$ $(20,9)$
56	$(20,36)$	$(20,16)$ $(25,6)$
64		$(4,56)$ $(30,4)$
72	$(16,56)$ $(30,42)$ $(36,36)$	$(4,64)$ $(30,12)$ $(36,0)$
81	$(9,72)$ $(25,56)$	$(16,49)$ $(36,9)$
90	$(9,81)$	$(9,72)$ $(30,30)$ $(42,6)$
100	$(36,64)$	$(42,16)$ $(49,2)$

Proof of $c = 2a + b$ for quarter-squares

If $t(n) = \lfloor (n+1)^2/4 \rfloor$,

$$\begin{aligned}
t(6n+0) &= 2t(4n) + t(2n-2)\\
t(6n+1) &= 2t(4n) + t(2n+1)\\
t(6n+2) &= 2t(4n+1) + t(2n)\\
t(6n+3) &= 2t(4n+2) + t(2n-1)\\
t(6n+4) &= 2t(4n+2) + t(2n+2)\\
t(6n+5) &= 2t(4n+3) + t(2n+1).
\end{aligned}$$

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

The increasing map

$$c \to \sqrt{24c+1}.$$

is a bijection between the pentagonal numbers $P(n) = (3n^2 - n)/2, n \in \mathbb{Z}$ and the positive integers coprime to 6.

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

The increasing map

$$c \to \sqrt{24c + 1}.$$

is a bijection between the pentagonal numbers $P(n) = (3n^2 - n)/2, n \in \mathbb{Z}$ and the positive integers coprime to 6.

The existence of a solution $c = 2a + b$ is equivalent to: for $z \geq 11$ coprime to 6, there are positive x and y coprime to 6 such that

$$z^2 + 2 = 2x^2 + y^2$$

other than the trivial solution $(x, y) = (1, z)$.

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Solutions of $k = 2x^2 + y^2$ correspond to elements $x\sqrt{-2} + y$ with norm k in the ring of integers $\mathbb{Z}[\sqrt{-2}]$ of $\mathbb{Q}(\sqrt{-2})$. Standard methods allow counting solutions via the prime factorization of k.

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Solutions of $k = 2x^2 + y^2$ correspond to elements $x\sqrt{-2} + y$ with norm k in the ring of integers $\mathbb{Z}[\sqrt{-2}]$ of $\mathbb{Q}(\sqrt{-2})$. Standard methods allow counting solutions via the prime factorization of k.

We can show that if $k = z^2 + 2$ has at least two distinct prime factors, there must be at least two solutions (with x, y positive and coprime to 6): the trivial $(x, y) = (1, z)$, and at least one that is nontrivial.

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Solutions of $k = 2x^2 + y^2$ correspond to elements $x\sqrt{-2} + y$ with norm k in the ring of integers $\mathbb{Z}[\sqrt{-2}]$ of $\mathbb{Q}(\sqrt{-2})$. Standard methods allow counting solutions via the prime factorization of k.

We can show that if $k = z^2 + 2$ has at least two distinct prime factors, there must be at least two solutions (with x, y positive and coprime to 6): the trivial $(x, y) = (1, z)$, and at least one that is nontrivial.

Note that k is always divisible by 3. Therefore, a second solution is guaranteed to exist unless k is a power of 3 (other than $k = 3$ and $k = 27$).

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Proposition: The only solutions of $3^n = x^2 + 2$ with $x, n \geq 0$ are $(n, x) = (1, 1)$ and $(3, 5)$.

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Proposition: The only solutions of $3^n = x^2 + 2$ with $x, n \geq 0$ are $(n, x) = (1, 1)$ and $(3, 5)$.

After ruling out various cases, this becomes

$$-2 = x^2 - 243y^2$$

This Pell-type equation can be solved explicitly. All the solutions (up to signs) are given by $x_0 = 265, y_0 = 17$, and for $k \geq 1$,

$$\begin{aligned} x_k &= 70226x_{k-1} + 1094715y_{k-1} \\ y_k &= 4505x_{k-1} + 70226y_{k-1} \end{aligned}$$

Proof of $c = 2a + b$ for pentagonal numbers (sketch)

Proposition: The only solutions of $3^n = x^2 + 2$ with $x, n \geq 0$ are $(n, x) = (1, 1)$ and $(3, 5)$.

After ruling out various cases, this becomes

$$-2 = x^2 - 243y^2$$

This Pell-type equation can be solved explicitly. All the solutions (up to signs) are given by $x_0 = 265, y_0 = 17$, and for $k \geq 1$,

$$\begin{aligned} x_k &= 70226x_{k-1} + 1094715y_{k-1} \\ y_k &= 4505x_{k-1} + 70226y_{k-1} \end{aligned}$$

One sees that every y_k is divisible by 17, and therefore cannot be a power of 3.

Alternative proof

Hirschhorn (2009) shows that the number of ways an integer c can be written as $2a + b$ with a, b pentagonal numbers is

$$d_{1,8}(24c+3) - d_{7,8}(24c+3) - \big(d_{1,8}((8c+1)/3) - d_{7,8}((8c+1)/3)\big),$$

where $d_{i,j}$ counts the number of positive divisors that are $i \pmod{j}$ for integral arguments, and equals 0 for non-integral rational arguments.

That this is ≥ 1 when c is pentagonal and $a, b < c$ can be shown using quadratic reciprocity and the proposition on the previous slide (we still need a similar amount of calculations).

Using less than n multiplications

Theorem: For any integer-valued quadratic polynomial $F(X)$,

$$\sum_{i=0}^{n} q^{F(i)}$$

can be computed using

$$O(n/\log^r n)$$

multiplications, for any $r > 0$.

Rectangular splitting

Paterson-Stockmeyer, 1973: method for evaluating *dense* series:

$$\sum_{k=0}^{N} \square q^k =$$

$$\begin{aligned} & (\square + \square q + \square q^2 + \ldots + \square q^{m-1}) \\ +q^m & (\square + \square q + \square q^2 + \ldots + \square q^{m-1}) \\ +q^{2m} & (\square + \square q + \square q^2 + \ldots + \square q^{m-1}) \\ +q^{3m} & (\square + \square q + \square q^2 + \ldots + \square q^{m-1}) \\ & \vdots \end{aligned}$$

Cost is $m + N/m$ multiplications, or $O(N^{1/2})$ with $m \sim N^{1/2}$.

No improvement for our sparse series with $n = O(N^{1/2})$ terms.

Rectangular splitting

Idea: choose m such that $F(X)$ takes few distinct values mod m.

Consider $F(X) = X^2$ and

$$s(m) = \text{number of squares mod } m$$

Rectangular splitting

Idea: choose m such that $F(X)$ takes few distinct values mod m.

Consider $F(X) = X^2$ and

$$s(m) = \text{number of squares mod } m$$

We need $O(s(m)\log m + N/m)$ multiplications, where we want m large and $s(m)$ small.

Rectangular splitting

Idea: choose m such that $F(X)$ takes few distinct values mod m.

Consider $F(X) = X^2$ and

$$s(m) = \text{number of squares mod } m$$

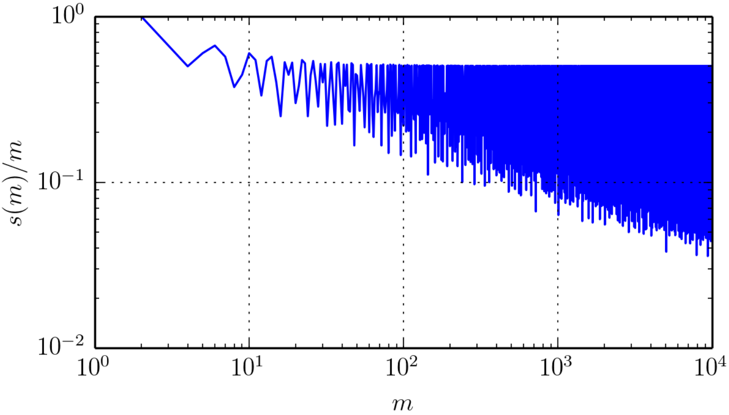
We need $O(s(m) \log m + N/m)$ multiplications, where we want m large and $s(m)$ small.

This suggests looking for m such that

$$\frac{s(m)}{m}$$

is small.

Successive minima



The m such that $s(m)/m < s(m')/m'$ for all $m' < m$ are a good choice.

k	$m = \text{A085635}(k)$	$s(m) = \text{A084848}(k)$	$s(m)/m$
1	$2 = 2$	2	1.0
2	$3 = 3$	2	0.67
3	$4 = 2^2$	2	0.50
4	$8 = 2^3$	3	0.38
5	$12 = 2^2 \cdot 3$	4	0.33
6	$16 = 2^4$	4	0.25
7	$32 = 2^5$	7	0.22
8	$48 = 2^4 \cdot 3$	8	0.17
9	$80 = 2^4 \cdot 5$	12	0.15
10	$96 = 2^5 \cdot 3$	14	0.15
11	$112 = 2^4 \cdot 7$	16	0.14
12	$144 = 2^4 \cdot 3^2$	16	0.11
13	$240 = 2^4 \cdot 3 \cdot 5$	24	0.10
14	$288 = 2^5 \cdot 3^2$	28	0.097
15	$336 = 2^4 \cdot 3 \cdot 7$	32	0.095
16	$480 = 2^5 \cdot 3 \cdot 5$	42	0.088

k	m	$s(m)$	$s(m)/m$
17	$560 = 2^4 \cdot 5 \cdot 7$	48	0.086
18	$576 = 2^6 \cdot 3^2$	48	0.083
19	$720 = 2^4 \cdot 3^2 \cdot 5$	48	0.067
20	$1008 = 2^4 \cdot 3^2 \cdot 7$	64	0.063
21	$1440 = 2^5 \cdot 3^2 \cdot 5$	84	0.058
22	$1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$	96	0.057
23	$2016 = 2^5 \cdot 3^2 \cdot 7$	112	0.056
24	$2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$	144	0.055
25	$2880 = 2^6 \cdot 3^2 \cdot 5$	144	0.050
26	$3600 = 2^4 \cdot 3^2 \cdot 5^2$	176	0.049
27	$4032 = 2^6 \cdot 3^2 \cdot 7$	192	0.048
28	$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	192	0.038
	$\vdots$		
94	$41801760 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	211680	0.0051
95	$42325920 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$	211680	0.0050
96	$48454560 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23$	241920	0.0050
97	$49008960 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	217728	0.0044
98	$54774720 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	241920	0.0044
99	$61261200 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	266112	0.0043
100	$68468400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	295680	0.0043

The function $s(m)$ is multiplicative, and takes the values

$$s(m) = \begin{cases} \frac{1}{2}p^e - \frac{1}{2}p^{e-1} + \frac{p^{e-1} - p^{(e+1) \bmod 2}}{2(p+1)} + 1 & \text{for } p \text{ odd;} \\ 2 & \text{for } p = 2 \text{ and } e \leq 2; \\ 2^{e-3} + \frac{2^{e-3} - 2^{(e+1) \bmod 2}}{3} + 2 & \text{for } p = 2 \text{ and } e \geq 3, \end{cases}$$

at prime powers $m = p^e$.

The function $s(m)$ is multiplicative, and takes the values

$$s(m) = \begin{cases} \frac{1}{2}p^e - \frac{1}{2}p^{e-1} + \frac{p^{e-1} - p^{(e+1) \bmod 2}}{2(p+1)} + 1 & \text{for } p \text{ odd;} \\ 2 & \text{for } p = 2 \text{ and } e \leq 2; \\ 2^{e-3} + \frac{2^{e-3} - 2^{(e+1) \bmod 2}}{3} + 2 & \text{for } p = 2 \text{ and } e \geq 3, \end{cases}$$

at prime powers $m = p^e$.

Minimizing $s(m) \log m + N/m$ under the assumption that m is a product of distinct primes gives the bound in the theorem.

The function $s(m)$ is multiplicative, and takes the values

$$s(m) = \begin{cases} \frac{1}{2}p^e - \frac{1}{2}p^{e-1} + \frac{p^{e-1} - p^{(e+1) \bmod 2}}{2(p+1)} + 1 & \text{for } p \text{ odd;} \\ 2 & \text{for } p = 2 \text{ and } e \leq 2; \\ 2^{e-3} + \frac{2^{e-3} - 2^{(e+1) \bmod 2}}{3} + 2 & \text{for } p = 2 \text{ and } e \geq 3, \end{cases}$$

at prime powers $m = p^e$.

Minimizing $s(m) \log m + N/m$ under the assumption that m is a product of distinct primes gives the bound in the theorem.

The construction is analogous for other quadratic polynomials.

Successive minima for trigonal numbers

k	m	$t(m)$	$t(m)/m$
1	$2 = 2$	1	0.50
2	$6 = 2 \cdot 3$	2	0.33
3	$10 = 2 \cdot 5$	3	0.30
4	$14 = 2 \cdot 7$	4	0.29
5	$18 = 2 \cdot 3^2$	4	0.22
6	$30 = 2 \cdot 3 \cdot 5$	6	0.20
7	$42 = 2 \cdot 3 \cdot 7$	8	0.19
8	$66 = 2 \cdot 3 \cdot 11$	12	0.18
9	$70 = 2 \cdot 5 \cdot 7$	12	0.17
10	$90 = 2 \cdot 3^2 \cdot 5$	12	0.13
	$\vdots$		
100	$25160850 = 2 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	199584	0.0079
101	$25675650 = 2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	203280	0.0079
102	$28120950 = 2 \cdot 3^2 \cdot 5^2 \cdot 11 \cdot 13 \cdot 19 \cdot 23$	221760	0.0079
103	$29099070 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	181440	0.0062

Successive minima for pentagonal numbers

k	m	$p(m)$	$p(m)/m$
1	$2 = 2$	2	1.0
2	$5 = 5$	3	0.60
3	$7 = 7$	4	0.57
4	$11 = 11$	6	0.55
5	$13 = 13$	7	0.54
6	$17 = 17$	9	0.53
7	$19 = 19$	10	0.53
8	$23 = 23$	12	0.52
9	$25 = 5^2$	11	0.44
10	$35 = 5 \cdot 7$	12	0.34
	$\vdots$		
100	$4555915 = 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 31$	120960	0.027
101	$5159245 = 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	136080	0.026
102	$5311735 = 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	136080	0.026
103	$6697405 = 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29$	170100	0.025

Example: computing θ_3

Suppose we want to compute

$$1 + 2\sum_{k=1}^{n} q^{k^2} \approx 1 + \sum_{k=1}^{\infty} 2q^{k^2}$$

for $q = \exp(-\pi)$, with n such that the error is less than 2^{-B}

Example: computing θ_3

Suppose we want to compute

$$1 + 2\sum_{k=1}^{n} q^{k^2} \approx 1 + \sum_{k=1}^{\infty} 2q^{k^2}$$

for $q = \exp(-\pi)$, with n such that the error is less than 2^{-B}

B	n	$\#(n^2)$	m	$s(m)$	$\#(\mathrm{mod}\ m)$	$\#(\mathrm{tot})$	Speedup
10^3	14	23	48	8	12	16	1.44
10^4	46	71	144	16	23	37	1.92
10^5	148	228	720	48	57	87	2.62
10^6	469	690	1680	96	109	239	2.89
10^7	1485	2098	10080	336	356	574	3.66

$\#(n^2)$: number of additions to generate $1, 4, 9, \ldots, n^2$
$\#(\mathrm{mod}\ m)$: number of additions to generate $1, 4, 9, \ldots \bmod m$
$\#(\mathrm{tot})$: total multiplications in the rectangular splitting algorithm

The end