An unusual primality test

Ben North

November 5, 2012

1 The Computist Quiz

The following programming problem is one of several on a freely-available set of interesting questions [3]:

> **Amphibious Discursion.** *A predicate on positive integers:*
>
> ```
> boolean isToad(int n)
> {
>   return ((n == 2)
>           || (n == frog(4, floor((n - 1) / 2), 1, 0) - 1));
> }
> ```
>
> *is defined with the aid of the following helper method:*
>
> ```
> int frog(int q, int r, int s, int t)
> {
>   if (r < t)
>     return 0;
>   else if (r == t)
>     return 1;
>   else if (q == 0)
>     return 0;
>   else
>     return (frog(q, r, s + 1, s + t)
>             + frog(q - 1, r - t, 1, 0));
> }
> ```
>
> *Which integers are toads? Describe what the* `frog` *method does. Can you explain why this code works?*

1.1 Analysis of the function `frog`

After some experimentation, we can form and prove the following conjectures:

1.1.1 Argument r is never negative

We prove this by induction on the call-stack depth. The specification says that `isToad` is a predicate on positive integers, so we have that $n > 0$ within `isToad`. Therefore

$$\left\lfloor \frac{n-1}{2} \right\rfloor \geq 0$$

and we have the base case.

Otherwise, the immediate caller of `frog` is again `frog`, and by the inductive hypothesis, $r \geq 0$ there. The first recursive call, receiving the same r, therefore satisfies the hypothesis. By the time we have reached the recursive calls, we have $r > t$. (The other two cases, $r = t$ and $r < t$, lead to an early `return`.) Therefore $r - t > 0$ and the hypothesis is satisfied for the second recursive call also.

1.1.2 Argument t to `frog` receives triangular numbers

The triangular numbers are

$$T_0 = 0; \quad T_1 = 1; \quad T_2 = 3; \quad T_3 = 6; \quad \ldots,$$

and in general

$$T_n = \frac{1}{2} n(n+1).$$

We claim that in all calls to `frog`, the argument t is the triangular number T_n, where $s = n + 1$. We prove this by induction on the call-stack depth.

Base case: If there is only one call to `frog`, then the immediate caller must have been `isToad`, and the arguments it supplies to `frog` are $t = 0 = T_0$ and $s = 1 = 0 + 1$, so the claim is true in this base case.

Inductive step: For deeper call stacks, the immediate caller is `frog`, and in the calling frame, by the inductive hypothesis, we have $t = T_n$ and $s = n + 1$ for some n. We look at the two recursive calls to `frog` separately:

- `frog(q, r, s + 1, s + t)`

  Writing s' and t' for the values of the arguments s and t received by this invocation of `frog`, we have

  $$\begin{aligned} s' &= s + 1 = n + 2; \\ t' &= t + s = T_n + (n+1) = T_{n+1}. \end{aligned}$$

  The claim is true, with $n' = n + 1$.

- `frog(q - 1, r - t, 1, 0)`
  Here, $t = 0$ and $s = 1$, as in the base case; the claim is true.

1.1.3 Function `frog` counts sums of q triangular numbers

Under the conditions established by the previous observation, the claim is that `frog(q, r, s, t)` is the number of ordered q-tuples of triangular numbers such that the sum of the elements of the tuple is r, and such that the first element of the tuple is at least t.

When q is zero First note that the only way we can get a call with $q = 0$ is via the second recursive call within `frog`. (The original call, from `toad`, passes $q = 4$. The first recursive call cannot have $q = 0$ because the third early `return` would have been triggered if so.)

In the second recursive call, t receives 0. We know $r \geq 0$, so `frog` returns 1 exactly when $r = t = 0$ (via the second `if`); otherwise the third `if` causes `frog` to return 0. Note that we never reach the recursive calls if $q = 0$.

This satisfies the claim — the empty sum is the one and only way to express zero as a sum of zero triangular numbers, and there is no way to express any $r > 0$ as an empty sum.

When q is positive The structure of the code reflects the following argument for counting the number of ways of writing r as a sum of q triangular numbers such that the first one is at least t:

- If $r < t$, then there are no such sums.
- If $r = t$, then there is exactly one such sum, namely

  $$r = t + 0 + 0 + \cdots + 0,$$

  where there are $(q - 1)$ zeros. (Including possibly no zeros, if $q = 1$; recall here we are considering positive q.)
- If $r > t$, then we partition the set of q-term sums whose first term is at least t into two disjoint sets. In the following, all x_i are always triangular numbers. We have:

$$\begin{aligned}\{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 \geq t\} \\ = \{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 > t\} \\ \cup \{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 = t\}.\end{aligned}$$

Because $t = T_n$ for some triangular number T_n (in fact $n = s - 1$), and x_1 must be a triangular number also, $x_1 > t = T_n$ iff $x_1 \geq T_{n+1}$, and so the first set on the RHS can be written

$$\begin{aligned}\{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 > T_n\} \\ = \{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 \geq T_{n+1}\}.\end{aligned}$$

Its size is therefore calculated by the first recursive call:

```
frog(q, r, s + 1, s + t)
```

because $t + s$ gives the next triangular number after t, as shown in §1.1.2.

In counting the elements of the second set,

$$\{(x_1, x_2, \ldots, x_q) : \textstyle\sum x_i = r \text{ and } x_1 = t\},$$

we are looking for sums of the form

$$r = t + x_2 + \cdots + x_q,$$

i.e.,

$$r - t = x_2 + \cdots + x_q,$$

where there are now $q - 1$ terms on the RHS, with no restriction on the first term. Equivalently, we require that the first term is at least zero. Such sums are counted by the second recursive call

```
frog(q - 1, r - t, 1, 0).
```

To formally demonstrate that the recursion terminates would require induction over q and an inner induction over $r - t$, but the nub of the argument is captured by considering the two recursive calls separately:

- `frog(q, r, s + 1, s + t)`

  Because r remains fixed, and t receives consecutive triangular numbers, there will come a call when $t = T_n \geq r$, at which point one of the first two `return` clauses will be hit.

- `frog(q - 1, r - t, 1, 0)`

  Here, q decreases by one on each recursive call, and so there will come a call when $q = 0$, at which point the third `return` clause will be hit.

Both recursions will therefore terminate.

1.1.4 Result of call to `frog` within `isToad`

We introduce the notation

$$t_k(n) = \text{number of } k\text{-tuples } (x_1, x_2, \ldots, x_k) \text{ such that each } x_i \text{ is a triangular number and } \textstyle\sum x_i = n.$$

for the concept 'how many ways n can be written as a sum of k triangular numbers'. In counting the ways, the order of the sum matters. For example, when finding $t_2(4)$, the sums $1 + 3$ and $3 + 1$ are counted separately.

The call to `frog` within `isToad` therefore computes

$$\texttt{frog(4, floor((n - 1) / 2), 1, 0)} = t_4\left(\left\lfloor \frac{n-1}{2} \right\rfloor\right)$$

because the argument $t = 0$ places no restrictions on the size of the first triangular number in the sums.

1.2 Analysis of the function `isToad`

We can now understand what the predicate `isToad` does — it is true for the special case $n = 2$, or for those n satisfying

$$n = t_4\left(\left\lfloor \frac{n-1}{2} \right\rfloor\right) - 1. \tag{1}$$

1.3 Empirical study of integers satisfying `isToad`

On writing and running a program to test whether `isToad` holds for integers $n = 1, 2, \ldots$, we find that `isToad`(n) is true for

$$n \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\},$$

strongly suggesting that `isToad`(n) holds exactly when n is prime. This is surprising, as there is no *prima facie* reason why counting sums of four triangular numbers should be in any way connected with primality.

2 Evaluation of $t_4(n)$

The key to understanding the behaviour of `isToad` is the following result:

$$t_4(n) = \sigma(2n + 1), \tag{2}$$

where $\sigma(m)$ is the sum of all (positive) divisors of m:

$$\sigma(m) = \sum_{d|m} d.$$

The bulk of this note reproduces a proof of this result, but we now use it to explain why `isToad` tests primality. We prove that

$$n = t_4\left(\left\lfloor \frac{n-1}{2} \right\rfloor\right) - 1 \quad \equiv \quad n \text{ is prime.}$$

2.1 Special values of n

Within `isToad`, the special case of $n = 2$ is first correctly handled. The specification also notes that $n > 0$, so we next check the other special case, namely $n = 1$. For this value of n,

$$\left\lfloor \frac{n-1}{2} \right\rfloor = 0,$$

so the test (1) is

$$1 =^? t_4(0) - 1$$

and, by (2), we have $t_4(0) = \sigma(1) = 1$, because the only factor of 1 is 1. (To check, there is exactly one way of writing zero as a sum of four triangular numbers, namely $0 = 0 + 0 + 0 + 0$.) The test therefore becomes $1 =^? 0$, which yields `false`. The non-primality of 1 is correctly assessed.

2.2 General even n

Now suppose that n is even, and $n > 2$. We must establish that `isToad` returns `false` for such n.

We have $\lfloor (n-1)/2 \rfloor = (n/2) - 1$, and so the test (1) is

$$n =^? t_4\big((n/2) - 1\big) - 1$$

i.e., by (2),

$$n =^? \sigma(n-1) - 1. \tag{3}$$

Now $n - 1$ is odd, and so might be prime. We consider the cases:

2.2.1 Composite $n - 1$

Suppose that $n - 1$ is not prime. In particular then, $n - 1 \geq 9$. Let p be the smallest prime factor of $n - 1$; we must have $3 \leq p < n - 1$. (Because $n - 1$ is odd, its smallest prime factor cannot be 2.) Then, because 1 and $n - 1$ are also distinct factors of $n - 1$,

$$\sigma(n-1) \geq 1 + 3 + (n-1) = n + 3,$$

and the RHS of (3) satisfies

$$\sigma(n-1) - 1 \geq n + 2 > n,$$

so $n \neq \sigma(n-1) - 1$, and the test (3) yields `false`, as required.

2.2.2 Prime $n - 1$

If, on the other hand, $n - 1$ is prime, then its factors are just 1 and $n - 1$, so $\sigma(n-1) = n$, and the test (3) becomes

$$n \stackrel{?}{=} n - 1,$$

which yields `false`, as required.

2.3 General odd n

For n odd with $n > 1$, we have $\lfloor (n-1)/2 \rfloor = (n-1)/2$, so the test is

$$\begin{aligned} & n \stackrel{?}{=} t_4\big((n-1)/2\big) - 1 \\ \equiv \quad & n \stackrel{?}{=} \sigma(n) - 1. \end{aligned} \tag{4}$$

Again, we consider the cases of prime and composite n separately.

2.3.1 Composite n

Having dealt with the special case $n = 1$, suppose n is odd and composite; so in particular $n \geq 9$. Then its smallest prime factor p must satisfy $3 \leq p < n$; then n has distinct factors 1, p, and n (and probably others), and the same argument as in §2.2.1 shows that the test (4) gives `false`, as required.

2.3.2 Prime n

Finally, if n is prime, then its factors are just 1 and n, so $\sigma(n) = n + 1$, and the test (4) becomes

$$n \stackrel{?}{=} n$$

which yields `true`. This concludes the case analysis, and completes the explanation of `isToad`'s behaviour.

3 Source of following proof

The presentation of the proof for $t_4(n) = \sigma(2n+1)$ below follows directly that in Bruce C. Berndt's book *Number Theory in the Spirit of Ramanujan* [1]. I have extracted just the parts which are on the direct route to the result of interest, and added some working.

> Working is shown like this.

3.1 Justification of manipulations

As Berndt notes [1, p.9] in a particular case (interchanging a limit and an infinite sum), various manipulations which, to be fully rigorous, require justification, are carried out without such justification. We take the same approach in this note.

4 Infinite products

We use the following notation for certain infinite products:

$$(a;q)_\infty = \prod_{k=0}^{\infty}(1-aq^k) = (1-a)(1-aq)(1-aq^2)\cdots.$$

There are a couple of manipulations of such expressions which we will use:

Interleaving By taking factors in turn from $(q;q^2)_\infty$ and from $(q^2;q^2)_\infty$, we see $(q;q^2)_\infty(q^2;q^2)_\infty = (q;q)_\infty$.

$$\begin{array}{rlllllll}
(q;q^2)_\infty(q^2;q^2)_\infty = & (1-q) & & (1-q^3) & & (1-q^5) & & \cdots \\
\times & & (1-q^2) & & (1-q^4) & & (1-q^6) & \cdots \\
= & (1-q) & (1-q^2) & (1-q^3) & (1-q^4) & (1-q^5) & (1-q^6) & \cdots \\
= & (q;q)_\infty & & & & & &
\end{array} \tag{5}$$

Similar cases such as

$$\begin{aligned}
(-q;q^4)_\infty(-q^3;q^4)_\infty &= (-q;q^2)_\infty; \\
(q^2;q^4)_\infty(q^4;q^4)_\infty &= (q^2;q^2)_\infty
\end{aligned}$$

follow in the same way. We can represent the general case as

$$(\pm q^m;q^{2n})_\infty(\pm q^{m+n};q^{2n})_\infty = (\pm q^m;q^n)_\infty,$$

where all '$\pm$' take the same sign.

The argument can also be applied backwards, to 'de-interleave' one product into two.

Difference of squares By taking, in pairs, one factor from $(-q;q^2)_\infty$ and one from $(q;q^2)_\infty$, we see that the two products combine:

$$(-q;q^2)_\infty(q;q^2)_\infty = (q^2;q^4)_\infty. \tag{6}$$

$$\begin{aligned} (-q;q^2)_\infty(q;q^2)_\infty = &\quad (1+q)\,(1+q^3)\,(1+q^5)\,\cdots \\ &\times\ (1-q)\,(1-q^3)\,(1-q^5)\,\cdots \\ = &\quad (1-q^2)(1-q^6)(1-q^{10})\cdots \\ = &\ (q^2;q^4)_\infty \end{aligned}$$

Similar results can be demonstrated in the same way:

$$\begin{aligned} (-q^2;q^2)_\infty(q^2;q^2)_\infty &= (q^4;q^4)_\infty; \\ (-q^2;q^4)_\infty(q^2;q^4)_\infty &= (q^4;q^8)_\infty. \end{aligned}$$

The general result is

$$(-q^m;q^n)_\infty(q^m;q^n)_\infty = (q^{2m};q^{2n})_\infty,$$

and the argument can also apply backwards by factorising each difference of squares.

5 The Jacobi triple product identity

A central result is the Jacobi triple product identity:

$$(-qz;q^2)_\infty(-q/z;q^2)_\infty(q^2;q^2)_\infty = \sum_{n=-\infty}^{\infty} q^{n^2} z^n. \tag{7}$$

This is proved in Berndt's book [1, theorem 1.3.3], but the following proof is more direct; it is the one on Wikipedia, which gives Cameron [2] as its source.

Proof

By dividing by the $(q^2;q^2)_\infty$ factor, and then substituting $q \leftarrow q^{1/2}$, the Jacobi triple product identity can be expressed as

$$\prod_{n>0}(1+q^{n-1/2}z)(1+q^{n-1/2}z^{-1}) = \left(\sum_{n=-\infty}^{\infty} q^{n^2/2}z^n\right)\left(\prod_{n>0}(1-q^n)^{-1}\right).$$

and it is in this form that we prove it. To do so, we introduce the notion of the 'Dirac sea'.

The Dirac sea

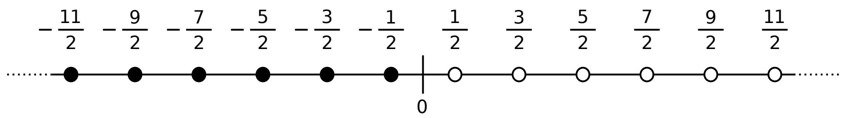
A ‘level’ is a half-integer, i.e., $n + 1/2$ for some $n \in \mathbb{Z}$. The ‘vacuum state’ is the set of all negative levels. A ‘state’ is a set of levels whose symmetric difference with the vacuum state is finite. The ‘energy’ of the state S is

$$\sum\{v \colon v > 0, v \in S\} - \sum\{v \colon v < 0, v \notin S\} \tag{8}$$

and the ‘particle count’ of S is

$$|\{v \colon v > 0, v \in S\}| - |\{v \colon v < 0, v \notin S\}|. \tag{9}$$

Each level can be thought of as a slot which can either hold a particle or not. A particle in level v has energy v, where negative energy levels are included. The vacuum state has particles in all the negative-energy slots:



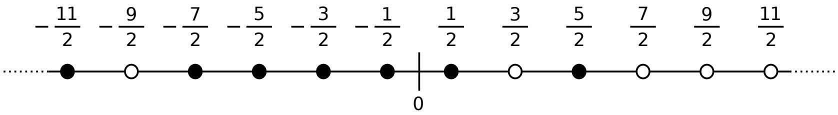
The ‘energy’ of a state S is how much more energy its particles have in total than the vacuum state; its particle count is how many more particles it has than the vacuum state. However, the vacuum state has infinite particle count and infinite negative energy, so the expressions (8) and (9) calculate the differences which at first sight are ‘$\infty - \infty$’.

Number of states with particle count l and energy m

An unordered choice of the presence of finitely many positive levels and the absence of finitely many negative levels (relative to the vacuum) corresponds to a state, so the generating function $\sum_{l,m} s(l,m)q^m z^l$ for the number $s(l,m)$ of states with particle count l and energy m can be expressed as

$$\sum_{l,m} s(l,m)q^m z^l = \prod_{n>0} (1 + q^{n-1/2}z)(1 + q^{n-1/2}z^{-1}).$$

For example, consider the state which, starting with the vacuum state, adds particles to levels $1/2$ and $5/2$, and removes the particle from level $-9/2$:



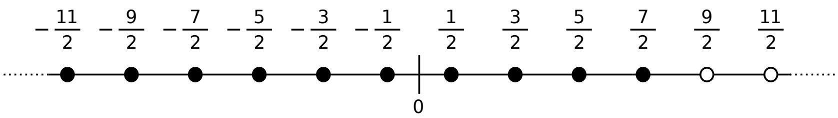
It has particle count $2 - 1 = 1$ and energy $1/2 + 5/2 - (-9/2) = 15/2$. It corresponds to choosing

- the $q^{1/2}z$ term from the $(1 + q^{1/2}z)$ factor;
- the $q^{5/2}z$ term from the $(1 + q^{5/2}z)$ factor;
- the $q^{9/2}z^{-1}$ term from the $(1 + q^{9/2}z^{-1})$ factor;
- and the 1 term from all other factors,

which multiply together to give $q^{15/2}z^1$. This choice will therefore contribute a count of one to the overall $q^{15/2}z^1$ term, whose coefficient will be the total number of states with energy $15/2$ and particle count 1.

On the other hand, consider the states with l particles; the minimum-energy such state has energy $l^2/2$.

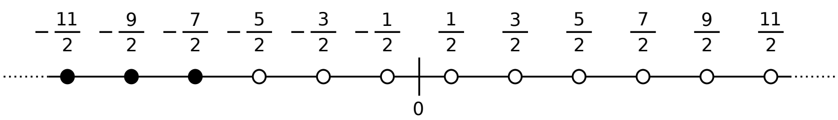
First take the case $l > 0$. The minimum-energy such state consists of placing particles in the lowest-energy l positive levels; for example, with $l = 4$:



The minimum-energy l-particle state therefore has energy

$$\frac{1}{2} + \frac{3}{2} + \cdots + \frac{2l-1}{2} = \frac{l^2}{2}.$$

A similar argument also applies for $l < 0$, where the minimum-energy state removes particles from the highest-energy (i.e., least negative) l negative levels. For example, the lowest-energy state having $l = -3$ is:



and the energy for general negative l is then given by the same calculation.

The case $l = 0$ is trivial — only the vacuum state itself has $l = 0$, and its energy is zero.

Now consider the set of l-particle states with energy m. We have $m \geq l^2/2$, and we put $n = m - l^2/2 \geq 0$. Each such state corresponds uniquely to a partition

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_j$$
$$\lambda_1 + \lambda_2 + \cdots + \lambda_j = n$$

of n into j pieces (for some j to be explained shortly) as follows:

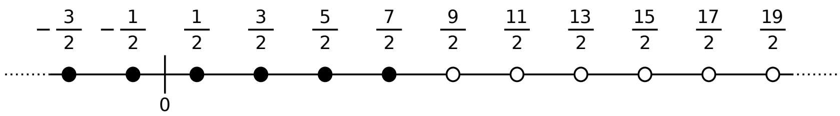
Given a partition of n, start with the minimum-energy state with l particles, as above. Move the highest-energy particle up by λ_1 levels (thereby increasing its energy by λ_1), the next highest particle up by λ_2 levels, and so on, down to the jth-highest particle, which is moved up λ_j levels. We have increased the energy by $\lambda_1 + \lambda_2 + \cdots + \lambda_j = n$, and so the resulting state has energy $m = n + l^2/2$. Thus j is the number of particles moved. The conditions

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_j$$

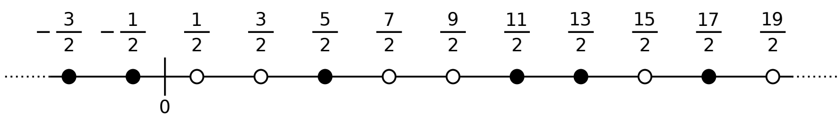
ensure that the particles neither 'overtake' nor 'land on top of' one another during this process.

In the other direction, from any l-particle state with energy m we can find the unique partition of $n = m - l^2/2$ which produces it under this mechanism.

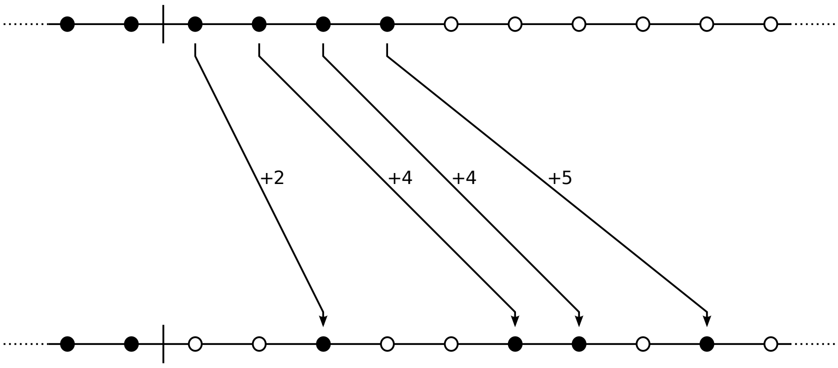
For example, consider the minimum-energy 4-particle state (note we have translated our view so as to see more of the positive levels):



It has energy 8, and can be transformed into the following 4-particle state with energy 23 (i.e., $n = 23 - 8 = 15$):



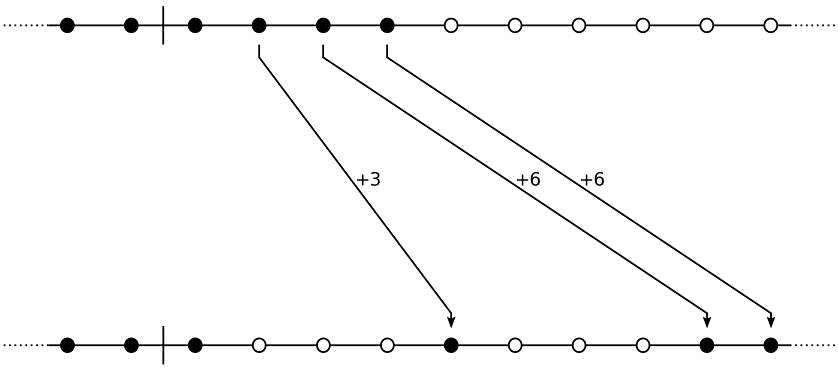
as follows:



which corresponds to the partition (taking the values from the highest-energy particle down)

$$5 + 4 + 4 + 2 = 15.$$

To take another example, the following 4-particle state, also with energy 23, corresponds to the partition $6 + 6 + 3 = 15$, and so involves moving up only the top three particles:



We can therefore count the states having l particles and energy $l^2/2 + n$ by counting the partitions of n. This is done by the partition function $p(n)$. The generating function $\sum_{l,m} s(l,m)q^m z^l$ can therefore be written

$$\sum_{l,m} s(l,m)q^m z^l = \sum_{l,n} p(n)q^{l^2/2+n}z^l = \left(\sum_{l=-\infty}^{\infty} q^{l^2/2}z^l\right)\left(\sum_{n\geq 0} p(n)q^n\right).$$

We now write the generating function for the partition function in its product form:

$$\sum_{n\geq 0} p(n)q^n = \prod_{k>0}(1-q^k)^{-1}.$$

> The factor $(1-q^k)^{-1}$ can be written $\sum_{j=0}^{\infty} q^{jk}$. Any given partition of n corresponds uniquely to a choice of one term from each such sum, where choosing q^{jk} corresponds to having j occurrences of the integer k in that partition of n. We will choose a term other than 1 from only finitely many of the sums.

Counting the states with particle count l and energy m this way, then,

$$\sum_{l,m} s(l,m)q^m z^l = \left(\sum_l q^{l^2/2} z^l\right)\left(\prod_{k>0}(1-q^k)^{-1}\right),$$

and equating the two expressions for $\sum_{l,m} s(l,m)q^m z^l$ gives Jacobi's triple product identity.

6 Generating square and triangular numbers

We define two generating functions; one which gives the square numbers and one which gives the triangular numbers:

$$\begin{aligned} \phi(q) &= \sum_{n=-\infty}^{\infty} q^{n^2} &&= \cdots + q^9 + q^4 + q + 1 + q + q^4 + q^9 + \cdots; \\ \psi(q) &= \sum_{n=0}^{\infty} q^{n(n+1)/2} &&= 1 + q + q^3 + q^6 + q^{10} + \cdots. \end{aligned}$$

The coefficient of q^m in $\phi(q)$ is the 'number of ways in which m is a square number'; e.g., the coefficient of q^4 is 2, because $4 = 2^2 = (-2)^2$. But there is at most one way an integer can be a triangular number in the definition of $\psi(q)$.

We also recall the notation

$$t_k(n) = \text{number of } k\text{-tuples of triangular numbers whose sum is } n,$$

and introduce

$$r_k(n) = \text{number of } k\text{-tuples of integers whose sum-of-squares is } n,$$

where the slightly convoluted definition of r_k gives the same 'double counting' as in $\phi(q)$.

The connection between r_k and ϕ, and between t_k and ψ, is that

$$[\phi(q)]^k = \phi^k(q) = \sum r_k(n)q^n; \quad [\psi(q)]^k = \psi^k(q) = \sum t_k(n)q^n.$$

6.1 Product forms

We can use the Triple Product Identity to find product forms for these. Setting $z = 1$ immediately gives us

$$\phi(q) = (-q; q^2)_\infty^2 (q^2; q^2)_\infty, \tag{10}$$

and with a little more work we find two representations for ψ:

$$\psi(q) = (-q; q^2)_\infty (q^4; q^4)_\infty \tag{11}$$

$$= \frac{(q^2; q^2)_\infty}{(q; q^2)_\infty}. \tag{12}$$

We find (11), the product expression for $\psi(q)$, by taking $q \leftarrow q^2$ and $z \leftarrow q^{-1}$ in (7). The RHS becomes

$$\sum_{n=-\infty}^{\infty} (q^2)^{n^2} (q^{-1})^n = \sum_{n=-\infty}^{\infty} q^{2n^2} q^{-n} = \sum_{n=-\infty}^{\infty} q^{n(2n-1)}.$$

Informally we see that this sum generates the triangular numbers:

n	$n(2n-1)$
-3	$21 = T_6$
-2	$10 = T_4$
-1	$3 = T_2$
0	$0 = T_0$
1	$1 = T_1$
2	$6 = T_3$
3	$15 = T_5$

More formally, break the sum into $\sum_{n=-\infty}^{\infty} = \sum_{n=-\infty}^{0} + \sum_{n=1}^{\infty}$. In the first, make the change of variable $n = -m$:

$$\sum_{n=-\infty}^{0} q^{n(2n-1)} = \sum_{m=0}^{\infty} q^{-m(-2m-1)} = \sum_{m=0}^{\infty} q^{(2m)(2m+1)/2} = \sum_{\substack{k=0\\k \text{ even}}}^{\infty} q^{k(k+1)/2},$$

and in the second, put $n = m + 1$:

$$\sum_{n=1}^{\infty} q^{n(2n-1)} = \sum_{m=0}^{\infty} q^{(m+1)(2m+1)} = \sum_{m=0}^{\infty} q^{(2m+2)(2m+1)/2}$$

$$= \sum_{m=0}^{\infty} q^{(2m+1)[(2m+1)+1]/2} = \sum_{\substack{k=0\\k \text{ odd}}}^{\infty} q^{k(k+1)/2},$$

Bring the 'even' and 'odd' sums back together to find:

$$\text{RHS} = \sum_{k=0}^{\infty} q^{k(k+1)/2} = \psi(q).$$

The LHS of the Jacobi triple product identity in this case is

$$(-q;q^4)_\infty(-q^3;q^4)_\infty(q^4;q^4)_\infty.$$

We interleave the first two factors, giving $(-q;q^2)_\infty$. We now have (11):

$$\psi(q) = (-q;q^2)_\infty(q^4;q^4)_\infty.$$

To transform this to the ratio form, (12), consider (11)'s first factor, $(-q;q^2)_\infty$. We have $(-q;q^2)_\infty(q;q^2)_\infty = (q^2;q^4)_\infty$, so $(-q;q^2)_\infty = (q^2;q^4)_\infty/(q;q^2)_\infty$. Now we can express $\psi(q)$ as

$$\psi(q) = \frac{(q^2;q^4)_\infty(q^4;q^4)_\infty}{(q;q^2)_\infty}.$$

Interleave the two factors on the top, giving $(q^2;q^2)_\infty$, to prove (12):

$$\psi(q) = \frac{(q^2;q^2)_\infty}{(q;q^2)_\infty}$$

7 Sums of two squares

Recall the notation

$$r_k(n) = \text{number of } k\text{-tuples } (x_1, x_2, \ldots, x_k) \text{ such that each } x_i \text{ is an integer and } \sum x_i^2 = n;$$

we also introduce the notation $d_{j,k}(n)$:

$$d_{j,k}(n) = \text{number of positive divisors } d \text{ of } n \text{ such that } d \equiv j \pmod{k}.$$

We can now count the number of ways to express an integer as the sum of two squares by means of the following theorem:

Theorem

$$r_2(n) = 4(d_{1,4}(n) - d_{3,4}(n)).$$

Proof

Put $q \leftarrow q^{1/2}$ and $z \leftarrow -a^2q^{1/2}$ in the Jacobi triple product identity to get

$$(a^2q;q)_\infty(a^{-2};q)_\infty(q;q)_\infty = \sum_{n=-\infty}^{\infty} q^{n^2/2}(-a^2q^{1/2})^n = \sum_{n=-\infty}^{\infty}(-1)^n a^{2n}q^{n(n+1)/2}.$$

In $(a^{-2};q)_\infty$, multiply by a, and pull out the first factor, $(1-a^{-2})$:

$$a(a^{-2};q)_\infty = (a-a^{-1})(a^{-2}q;q)_\infty$$

and hence

$$\begin{aligned}(a-a^{-1})(a^2q;q)_\infty(a^{-2}q;q)_\infty(q;q)_\infty &= a(a^2q;q)_\infty(a^{-2};q)_\infty(q;q)_\infty \\ &= \sum_{n=-\infty}^{\infty}(-1)^n a^{2n+1}q^{n(n+1)/2} \\ &= \left(\sum_{\substack{n=-\infty \\ n \text{ even}}}^{\infty} + \sum_{\substack{n=-\infty \\ n \text{ odd}}}^{\infty}\right)(-1)^n a^{2n+1}q^{n(n+1)/2}.\end{aligned}$$

Make the change of variables $n = 2m$ in the first sum, and $n = 2m-1$ in the second to get

$$\begin{aligned}&(a-a^{-1})(a^2q;q)_\infty(a^{-2}q;q)_\infty(q;q)_\infty \\ &\qquad = \sum_{m=-\infty}^{\infty} a^{4m+1}q^{m(2m+1)} - \sum_{m=-\infty}^{\infty} a^{4m-1}q^{m(2m-1)} \\ &\qquad = a(-a^4q^3;q^4)_\infty(-a^{-4}q;q^4)_\infty(q^4;q^4)_\infty \\ &\qquad\qquad - a^{-1}(-a^4q;q^4)_\infty(-a^{-4}q^3;q^4)_\infty(q^4;q^4)_\infty\end{aligned}$$

using the triple product identity two more times.

To evaluate $\sum_{m=-\infty}^{\infty} a^{4m+1}q^{m(2m+1)}$, put $z \leftarrow a^4q$ and $q \leftarrow q^2$ in the triple product identity. The 'sum' side is

$$\begin{aligned}\sum_{m=-\infty}^{\infty}(q^2)^{m^2}(a^4q)^m &= \sum_{m=-\infty}^{\infty} q^{2m^2}a^{4m}q^m \\ &= \sum_{m=-\infty}^{\infty} a^{4m}q^{2m^2+m} \\ &= a^{-1}\sum_{m=-\infty}^{\infty} a^{4m+1}q^{m(2m+1)},\end{aligned}$$

and the 'product' side is

$$(-a^4q^3;q^4)_\infty(-a^{-4}q;q^4)_\infty(q^4;q^4)_\infty.$$

To evaluate $\sum_{m=-\infty}^{\infty} a^{4m-1}q^{n(2m-1)}$, put $z \leftarrow a^4q^{-1}$ and $q \leftarrow q^2$. The 'sum' side is

$$\begin{aligned}\sum_{m=-\infty}^{\infty}(q^2)^{m^2}(a^4q^{-1})^m &= \sum_{m=-\infty}^{\infty} q^{2m^2}a^{4m}q^{-m}\\ &= \sum_{m=-\infty}^{\infty} a^{4m}q^{2m^2-m}\\ &= a\sum_{m=-\infty}^{\infty} a^{4m-1}q^{m(2m-1)},\end{aligned}$$

and the 'product' side is

$$(-a^4q;q^4)_\infty(-a^{-4}q^3;q^4)_\infty(q^4;q^4)_\infty.$$

The next step is to differentiate this with respect to a and then set $a=1$, by logarithmic differentiation. We need not actually carry out the differentiation of the infinite products on the LHS, because $(a-a^{-1})=0$ when $a=1$.

For example, to evaluate

$$\frac{\mathrm{d}}{\mathrm{d}a}\Big[(-a^4q^3;q^4)_\infty\Big]$$

we use

$$\frac{\mathrm{d}}{\mathrm{d}x}\Big[\log[f(x)]\Big] = \frac{1}{f(x)}f'(x); \qquad f'(x) = f(x)\frac{\mathrm{d}}{\mathrm{d}x}\Big[\log[f(x)]\Big].$$

In our example, this leads to

$$\begin{aligned}\log(-a^4q^3;q^4)_\infty &= \log(1+a^4q^3)+\log(1+a^4q^7)\\ &\quad+\log(1+a^4q^{11})+\cdots\\ \frac{\mathrm{d}}{\mathrm{d}a}\Big[\log(-a^4q^3;q^4)_\infty\Big] &= \frac{4a^3q^3}{1+a^4q^3}+\frac{4a^3q^7}{1+a^4q^7}+\frac{4a^3q^{11}}{1+a^4q^{11}}+\cdots\\ \frac{\mathrm{d}}{\mathrm{d}a}\Big[\log(-a^4q^3;q^4)_\infty\Big]\Big|_{a=1} &= \frac{4q^3}{1+q^3}+\frac{4q^7}{1+q^7}+\frac{4q^{11}}{1+q^{11}}+\cdots\\ &= \sum_{n=0}^{\infty}\frac{4q^{4n+3}}{1+q^{4n+3}}.\end{aligned}$$

The others are similar.

We obtain

$$
\begin{aligned}
2(q;q)_\infty^3 &= 2(-q^3;q^4)_\infty(-q;q^4)_\infty(q^4;q^4)_\infty \\
&\qquad + \Bigg[(-q^3;q^4)_\infty(-q;q^4)_\infty(q^4;q^4)_\infty \\
&\qquad\qquad \times \sum_{n=0}^{\infty}\left(\frac{4q^{4n+3}}{1+q^{4n+3}} - \frac{4q^{4n+1}}{1+q^{4n+1}} - \frac{4q^{4n+1}}{1+q^{4n+1}} + \frac{4q^{4n+3}}{1+q^{4n+3}}\right)\Bigg] \\
&= 2(-q^3;q^4)_\infty(-q;q^4)_\infty(q^4;q^4)_\infty \\
&\qquad \times \left[1 - 4\sum_{n=0}^{\infty}\left(\frac{q^{4n+1}}{1+q^{4n+1}} - \frac{q^{4n+3}}{1+q^{4n+3}}\right)\right].
\end{aligned}
$$

Now

$$
(-q^3;q^4)_\infty(-q;q^4)_\infty(q^4;q^4)_\infty = (-q;q)_\infty^2(q;q)_\infty
$$

We show this by a sequence of splitting and re-combining. Start by interleaving the factors to combine $(-q^3;q^4)_\infty(-q;q^4)_\infty = (-q;q^2)_\infty$, giving

$$
\text{LHS} = (-q;q^2)_\infty(q^4;q^4)_\infty.
$$

Then factorise the differences of squares $(q^4;q^4)_\infty = (-q^2;q^2)_\infty(q^2;q^2)_\infty$:

$$
\text{LHS} = (-q;q^2)_\infty(-q^2;q^2)_\infty(q^2;q^2)_\infty;
$$

interleave to combine $(-q;q^2)_\infty(-q^2;q^2)_\infty = (-q;q)_\infty$:

$$
\text{LHS} = (-q;q)_\infty(q^2;q^2)_\infty.
$$

Finally, factorise $(q^2;q^2)_\infty = (q;q)_\infty(-q;q)_\infty$ to reach the RHS.

so

$$
\frac{(q;q)_\infty^2}{(-q;q)_\infty^2} = 1 - 4\sum_{n=0}^{\infty}\left(\frac{4q^{4n+1}}{1+q^{4n+1}} - \frac{4q^{4n+3}}{1+q^{4n+3}}\right).
$$

Now

$$
\phi(-q) = (q;q^2)_\infty^2(q^2;q^2)_\infty = \frac{(q;q)_\infty}{(-q;q)_\infty} \tag{13}
$$

The first equality follows immediately from (10). To see the second, first interleave one of the $(q;q^2)_\infty$ and the $(q^2;q^2)_\infty$:

$$
(q;q^2)_\infty^2(q^2;q^2)_\infty = (q;q^2)_\infty(q;q)_\infty.
$$

We therefore show

$$(q;q^2)_\infty = \frac{1}{(-q;q)_\infty}.$$

From the interleaving $(q;q^2)_\infty(q^2;q^2)_\infty = (q;q)_\infty$, we have

$$(q;q^2)_\infty = \frac{(q;q)_\infty}{(q^2;q^2)_\infty},$$

and by factorising each difference of squares in $(q^2;q^2)_\infty$ we have

$$(q^2;q^2)_\infty = (q;q)_\infty(-q;q)_\infty,$$

and the result follows.

so, replacing q by $-q$, we see

$$\begin{aligned}\phi^2(q) &= 1 + 4\sum_{n=0}^{\infty}\left(\frac{q^{4n+1}}{1-q^{4n+1}} - \frac{q^{4n+3}}{1-q^{4n+3}}\right)\\ &= 1 + 4\sum_{m=0}^{\infty}\left(\sum_{r=1}^{\infty} q^{(4m+1)r} - \sum_{r=1}^{\infty} q^{(4m+3)r}\right)\end{aligned}$$

(where we have changed variable to $m = n$ in order to free n for the next step). Gather terms having the same power of q

We transform each of the two double sums into a single power series in q. Take the first sum, $\sum_{m=0}^{\infty}\sum_{r=1}^{\infty} q^{(4m+1)r}$. We would like to re-write this as $\sum_{n=0}^{\infty} a_n q^n$, and so have to find the values of the a_n. For a given n, which pairs (m,r) give a term $q^{(4m+1)r} = q^n$? Exactly those pairs having m such that $(4m+1)|n$, and each such m has exactly one corresponding r, and so contributes one to the coefficient a_n. Therefore, a_n is the number of $m \geq 0$ such that $(4m+1)|n$, i.e., the number of positive divisors d of n having $d = 1 \pmod 4$.

to find

$$\begin{aligned}\phi^2(q) &= 1 + 4\sum_{n=1}^{\infty}\left(\sum_{\substack{d|n\\ d\equiv 1 \pmod 4}} 1 - \sum_{\substack{d|n\\ d\equiv 3 \pmod 4}} 1\right) q^n\\ &= 1 + 4\sum_{n=1}^{\infty}\big(d_{1,4}(n) - d_{3,4}(n)\big)q^n. \qquad (14)\end{aligned}$$

Equating coefficients of powers in $\phi^2(k) = \sum r_2(n)q^n$ now gives the result.

8 Sums of four squares

To count the number of ways of expressing an integer as the sum of four squares, we use the following theorem:

Theorem

$$r_4(n) = 8 \sum_{\substack{d|n \\ 4\nmid d}} d.$$

The proof will start by using Jacobi's identity:

8.1 Jacobi's identity

The triple product identity with $z \leftarrow z^2 q$ gives

$$\sum_{n=-\infty}^{\infty} z^{2n} q^{n^2+n} = (-z^2q^2; q^2)_\infty (-1/z^2; q^2)_\infty (q^2; q^2)_\infty.$$

Divide both sides by $1 + 1/z^2$, which is the first factor in $(-1/z^2; q^2)_\infty$:

$$\frac{\sum_{n=-\infty}^{\infty} z^{2n} q^{n^2+n}}{1 + 1/z^2} = (-z^2q^2; q^2)_\infty (-q^2/z^2; q^2)_\infty (q^2; q^2)_\infty.$$

We now take the limit $z \to i$.

The idea is to 'put $z^2 = -1$', which will give the RHS the form we will use. The LHS, though, would be

$$\frac{\sum_{n=-\infty}^{\infty} (-1)^n q^{n^2+n}}{1-1}.$$

The bottom is zero, and we can see informally that the terms on the top cancel in pairs:

	n	$(-1)^n q^{n^2+n}$
$(m=2)$	-3	$-q^6$
$(m=1)$	-2	$+q^2$
$(m=0)$	-1	$-q^0$
	0	$+q^0$
	1	$-q^2$
	2	$+q^6$

More formally, break the sum into $\sum_{n=-\infty}^{-1} + \sum_{n=0}^{\infty}$, and change variables in the first (as shown) to $n = -(m+1)$ to get

$$\begin{aligned}\sum_{n=-\infty}^{\infty}(-1)^n q^{n^2+n} &= \sum_{m=0}^{\infty}(-1)^{-(m+1)} q^{(m+1)^2-(m+1)} + \sum_{n=0}^{\infty}(-1)^n q^{n^2+n} \\ &= \sum_{m=0}^{\infty} -(-1)^m q^{m^2+m} + \sum_{n=0}^{\infty}(-1)^n q^{n^2+n} \\ &= 0. \end{aligned} \tag{15}$$

Instead of just setting $z = i$, then, we must take the limit $z \to i$.

To do so, use l'Hôpital's rule. First simplify slightly by multiplying top and bottom of the LHS by z:

$$\text{LHS} = \frac{\sum_{n=-\infty}^{\infty} z^{2n+1} q^{n(n+1)}}{z + z^{-1}}.$$

Now differentiate (with respect to z) top and bottom, cheerfully moving the $\mathrm{d}/\mathrm{d}z$ inside the sum:

$$\frac{\sum_{n=-\infty}^{\infty}(2n+1) z^{2n} q^{n(n+1)}}{1 - z^{-2}}$$

and evaluate at $z = i$ to find the limit of the LHS,

$$\frac{1}{2}\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)q^{n(n+1)}.$$

On the RHS we can just set $z = i$. Combining these, we have Jacobi's identity,

$$\frac{1}{2}\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)q^{n(n+1)} = (q^2; q^2)_\infty^3.$$

(Note that the 'main' form given in [1] is different, but it is the above form that we require for the following proof.)

Proof of sums-of-four-squares result

Take $q \leftarrow q^{1/2}$ in Jacobi's identity as just proved,

$$(q; q)_\infty^3 = \frac{1}{2}\sum_{n=-\infty}^{\infty}(-1)^n(2n+1)q^{n(n+1)/2},$$

and square both sides to get

$$(q;q)_\infty^6 = \frac{1}{4} \sum_{m,n=-\infty}^{\infty} (-1)^{m+n}(2m+1)(2n+1)q^{(m^2+n^2+m+n)/2}.$$

Split this sum into its positive and negative terms:

$$\begin{aligned}(q;q)_\infty^6 &= \frac{1}{4}\left(\sum_{\substack{m,n=-\infty\\ m+n \text{ even}}}^{\infty} + \sum_{\substack{m,n=-\infty\\ m+n \text{ odd}}}^{\infty}\right)(-1)^{m+n}(2m+1)(2n+1)q^{(m^2+n^2+m+n)/2}\\ &= \frac{1}{4}\left(\sum_{\substack{m,n=-\infty\\ m+n \text{ even}}}^{\infty} (2m+1)(2n+1)q^{(m^2+n^2+m+n)/2}\right.\\ &\qquad\left. - \sum_{\substack{m,n=-\infty\\ m+n \text{ odd}}}^{\infty} (2m+1)(2n+1)q^{(m^2+n^2+m+n)/2}\right).\end{aligned}$$

Make a change of variables in each sum. In the first ('$m+n$ even'), put

$$\begin{aligned} m &= r+s;\\ n &= r-s \end{aligned}$$

and in the second ('$m+n$ odd'), put

$$\begin{aligned} m &= r+s;\\ n &= s-r-1. \end{aligned}$$

In both cases, as (r,s) runs over all pairs of integers, the corresponding pair (m,n) runs over all pairs of integers subject to the evenness or oddness constraint.

For the 'even' case,

$$m = r+s; \quad n = r-s,$$

any given (r,s) certainly gives rise to a pair (m,n) of integers, and we have $m+n=2r$, which is even. Conversely, we can invert to find

$$r = \frac{m+n}{2}; \quad s = \frac{m-n}{2},$$

and if $m+n$ is even, then so is $m-n$, and hence r and s are both integers.

A similar argument applies for the 'odd' case.

We now have

$$
\begin{aligned}
(q;q)_\infty^6 &= \frac{1}{4}\Bigg(\sum_{r,s=-\infty}^{\infty} (2r+2s+1)(2r-2s+1)q^{r^2+s^2+r} \\
&\qquad\qquad - \sum_{r,s=-\infty}^{\infty} (2r+2s+1)(2s-2r-1)q^{r^2+s^2+r} \Bigg) \\
&= \frac{1}{2} \sum_{r,s=-\infty}^{\infty} \big((2r+1)^2-(2s)^2\big) q^{r^2+s^2+r} \\
&= \frac{1}{2} \left(\sum_{s=-\infty}^{\infty} q^{s^2} \sum_{r=-\infty}^{\infty} (2r+1)^2 q^{r^2+r} - \sum_{r=-\infty}^{\infty} q^{r^2+r} \sum_{s=-\infty}^{\infty} (2s)^2 q^{s^2} \right).
\end{aligned}
$$

The non-unity coefficients in the two power series $\sum(2r+1)^2q^{r^2+r}$ and $\sum(2s)^2q^{s^2}$ make this expression difficult to manipulate further, and so we re-write the two series using derivatives.

To get $\sum_{r=-\infty}^{\infty}(2r+1)^2q^{r^2+r}$ into a more workable form, we expand a term: $(4r^2+4r+1)q^{r^2+r} = (1+4(r^2+r))q^{r^2+r}$, then note that

$$
\frac{\mathrm{d}}{\mathrm{d}q}\left[q^{r^2+r}\right] = (r^2+r)q^{r^2+r-1}; \qquad 4q\frac{\mathrm{d}}{\mathrm{d}q}\left[q^{r^2+r}\right] = 4(r^2+r)q^{r^2+r}.
$$

Hence

$$
\sum_{r=-\infty}^{\infty} (2r+1)^2 q^{r^2+r} = \left(1+4q\frac{\mathrm{d}}{\mathrm{d}q}\right) \sum_{r=-\infty}^{\infty} q^{r^2+r}.
$$

Similarly, one term of $\sum_{s=-\infty}^{\infty}(2s)^2q^{s^2}$ is $4s^2q^{s^2}$, and

$$
\frac{\mathrm{d}}{\mathrm{d}q}\left[q^{s^2}\right] = s^2q^{s^2-1}; \qquad 4q\frac{\mathrm{d}}{\mathrm{d}q}\left[q^{s^2}\right] = 4s^2q^{s^2}
$$

so

$$
\sum_{s=-\infty}^{\infty} (2s)^2 q^{s^2} = \left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right) \sum_{s=-\infty}^{\infty} q^{s^2}.
$$

We have now reached

$$
\begin{aligned}
(q;q)_\infty^6 = \frac{1}{2}\Bigg(&\sum_{s=-\infty}^{\infty} q^{s^2} \left(1+4q\frac{\mathrm{d}}{\mathrm{d}q}\right) \sum_{r=-\infty}^{\infty} q^{r^2+r} \\
&- \sum_{r=-\infty}^{\infty} q^{r^2+r} \left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right) \sum_{s=-\infty}^{\infty} q^{s^2} \Bigg)
\end{aligned}
$$

and use

$$\sum_{s=-\infty}^{\infty} q^{s^2} = (-q;q^2)_\infty^2 (q^2;q^2)_\infty;$$
$$\sum_{r=-\infty}^{\infty} q^{r^2+r} = 2(-q^2;q^2)_\infty^2 (q^2;q^2)_\infty.$$

The first sum is just the definition of $\phi(q)$, which as shown in §6.1 has the given product form.

For the second sum, use $z \leftarrow q$ in the Jacobi triple product identity:

$$\begin{aligned}\sum_{r=-\infty}^{\infty} q^{r^2+r} &= \sum_{r=-\infty}^{\infty} q^{r^2} q^r \\ &= (-q^2;q^2)_\infty (-1;q^2)_\infty (q^2;q^2)_\infty.\end{aligned}$$

Now

$$\begin{aligned}(-1;q^2)_\infty &= (1+1)(1+q^2)(1+q^4)\cdots \\ &= 2(-q^2;q^2)_\infty,\end{aligned}$$

so

$$\sum_{r=-\infty}^{\infty} q^{r^2+r} = 2(-q^2;q^2)_\infty^2 (q^2;q^2)_\infty.$$

We have

$$\begin{aligned}(q;q)_\infty^6 = \frac{1}{2}\Bigg(&(-q;q^2)_\infty^2 (q^2;q^2)_\infty \left(1 + 4q\frac{\mathrm{d}}{\mathrm{d}q}\right) 2(-q^2;q^2)_\infty^2 (q^2;q^2)_\infty \\ &- 2(-q^2;q^2)_\infty^2 (q^2;q^2)_\infty \left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right) (-q;q^2)_\infty^2 (q^2;q^2)_\infty \Bigg) \\ = &(-q;q^2)_\infty^2 (q^2;q^2)_\infty \left(1 + 4q\frac{\mathrm{d}}{\mathrm{d}q}\right) (-q^2;q^2)_\infty^2 (q^2;q^2)_\infty \\ &- (-q^2;q^2)_\infty^2 (q^2;q^2)_\infty \left(4q\frac{\mathrm{d}}{\mathrm{d}q}\right) (-q;q^2)_\infty^2 (q^2;q^2)_\infty.\end{aligned}$$

Now logarithmically differentiate

For example, to differentiate $(-q^2;q^2)^2_\infty(q^2;q^2)_\infty$ w.r.t. q, using $f' = f[\log f]'$:

$$\begin{aligned}
\log\left[(-q^2;q^2)^2_\infty(q^2;q^2)_\infty\right] &= 2\log\left[(1+q^2)(1+q^4)(1+q^6)\cdots\right] \\
&\quad+\log\left[(1-q^2)(1-q^4)(1-q^6)\cdots\right] \\
&= 2\log(1+q^2)+2\log(1+q^4)+2\log(1+q^6)+\cdots \\
&\quad+\log(1-q^2)+\log(1-q^4)+\log(1-q^6)+\cdots \\
\Big[\log\left[(-q^2;q^2)^2_\infty(q^2;q^2)_\infty\right]\Big]' &= 2\frac{2q}{1+q^2}+2\frac{4q^3}{1+q^4}+2\frac{6q^4}{1+q^6}+\cdots \\
&\quad-\frac{2q}{1-q^2}-\frac{4q^3}{1-q^4}-\frac{6q^5}{1-q^6}-\cdots \\
&= 2\sum_{n=1}^\infty \frac{2nq^{2n-1}}{1+q^{2n}}-\sum_{n=1}^\infty\frac{2nq^{2n-1}}{1-q^{2n}}
\end{aligned}$$

to find

$$\begin{aligned}
&(q;q)^6_\infty \\
&\quad= (-q;q^2)^2_\infty(q^2;q^2)^2_\infty(-q^2;q^2)^2_\infty\left(1+8\sum_{n=1}^\infty\frac{2nq^{2n}}{1+q^{2n}}-4\sum_{n=1}^\infty\frac{2nq^{2n}}{1-q^{2n}}\right) \\
&\qquad-(-q^2;q^2)^2_\infty(q^2;q^2)^2_\infty(-q;q^2)^2_\infty\left(8\sum_{n=1}^\infty\frac{(2n-1)q^{2n-1}}{1+q^{2n-1}}-4\sum_{n=1}^\infty\frac{2nq^{2n}}{1-q^{2n}}\right) \\
&\quad= (-q^2;q^2)^2_\infty(q^2;q^2)^2_\infty(-q;q^2)^2_\infty\left(1-8\sum_{n=1}^\infty\left[\frac{(2n-1)q^{2n-1}}{1+q^{2n-1}}-\frac{2nq^{2n}}{1+q^{2n}}\right]\right).
\end{aligned}$$

Now divide both sides by

$$\begin{aligned}
(-q;q)^4_\infty(q;q)^2_\infty &= (-q;q)^2_\infty(q^2;q^2)^2_\infty \\
&= (-q;q^2)^2_\infty(-q^2;q^2)^2_\infty(q^2;q^2)^2_\infty
\end{aligned}$$

The first equality follows immediately from the difference of squares result $(-q;q)_\infty(q;q)_\infty = (q^2;q^2)_\infty$. For the second step, de-interleave $(-q;q)_\infty$ into $(-q;q^2)_\infty(-q^2;q^2)_\infty$.

to deduce

$$\frac{(q;q)^4_\infty}{(-q;q)^4_\infty} = 1-8\sum_{n=1}^\infty\left[\frac{(2n-1)q^{2n-1}}{1+q^{2n-1}}-\frac{2nq^{2n}}{1+q^{2n}}\right].$$

Substituting using (13), and replacing q by $-q$, we find

$$\begin{aligned}
\phi(q)^4 &= 1 + 8\sum_{n=1}^{\infty}\left[\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}} + \frac{2nq^{2n}}{1+q^{2n}}\right] \\
&= 1 + 8\sum_{n=1}^{\infty}\left[\frac{(2n-1)q^{2n-1}}{1-q^{2n-1}} + \frac{2nq^{2n}}{1-q^{2n}}\right] - 8\sum_{n=1}^{\infty}\left[\frac{2nq^{2n}}{1-q^{2n}} - \frac{2nq^{2n}}{1+q^{2n}}\right].
\end{aligned}$$

The first sum is just

$$\sum_{m=1}^{\infty}\frac{mq^m}{1-q^m}$$

with its terms written in pairs, and the terms in the second sum can be simplified to give

$$\begin{aligned}
\phi^4(q) &= 1 + 8\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n} - 8\sum_{n=1}^{\infty}\frac{4nq^{4n}}{1-q^{4n}} \\
&= 1 + 8\sum_{\substack{n=1 \\ 4\nmid n}}^{\infty}\frac{nq^n}{1-q^n} \\
&= 1 + 8\sum_{\substack{n=1 \\ 4\nmid n}}^{\infty} nq^n \sum_{m=0}^{\infty} q^{nm}.
\end{aligned}$$

We now rearrange slightly and rename n to d

$$\begin{aligned}
\sum_{\substack{n=1 \\ 4\nmid n}}^{\infty} nq^n \sum_{m=0}^{\infty} q^{nm} &= \sum_{\substack{n=1 \\ 4\nmid n}}^{\infty}\sum_{m=0}^{\infty} nq^{n(m+1)} \\
&= \sum_{\substack{n=1 \\ 4\nmid n}}^{\infty}\sum_{m=1}^{\infty} nq^{nm} = \sum_{m=1}^{\infty}\sum_{\substack{n=1 \\ 4\nmid n}}^{\infty} nq^{nm} = \sum_{m=1}^{\infty}\sum_{\substack{d=1 \\ 4\nmid d}}^{\infty} dq^{dm}
\end{aligned}$$

to find

$$\phi^4(q) = 1 + 8\sum_{m=1}^{\infty}\sum_{\substack{d=1 \\ 4\nmid d}}^{\infty} dq^{dm}.$$

Introduce a new n by writing $n = dm$, and collect all terms in q^n together

There will be a contribution of d to the q^n term whenever $dm = n$ and $4 \nmid d$. The overall q^n term then has coefficient

$$\sum \Big\{ d : (d \geq 1) \text{ and } (\exists m \geq 1 : dm = n) \text{ and } (4 \nmid d) \Big\}.$$

The second clause here is just '$d \mid n$', which in the context of the sum implicitly includes the condition '$d \geq 1$', so the double sum becomes

$$\sum_{n=1}^{\infty} \sum_{\substack{d \mid n \\ 4 \nmid d}} d q^n.$$

to conclude

$$\phi^4(q) = 1 + \sum_{n=1}^{\infty} \left(8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d \right) q^n. \tag{16}$$

Equating powers of q gives the result.

9 Some identities involving ϕ and ψ

We have

$$\phi(q) + \phi(-q) = 2\phi(q^4); \tag{17}$$

$$\phi(q) - \phi(-q) = 4q\psi(q^8); \tag{18}$$

$$\phi(q)\psi(q^2) = \psi^2(q). \tag{19}$$

(The last one has a natural counting interpretation and a bijective/enumerative proof, which may be the subject of a future note.)

To show (17) is fairly straightforward, using the infinite sum form:

$$\begin{aligned}
\phi(q) + \phi(-q) &= \sum_{n=-\infty}^{\infty} q^{n^2} + \sum_{n=-\infty}^{\infty} (-q)^{n^2} \\
&= \sum_{n \text{ even}} \left[q^{n^2} + (-q)^{n^2} \right] + \sum_{n \text{ odd}} \left[q^{n^2} + (-q)^{n^2} \right]
\end{aligned}$$

The exponent n^2 is odd or even exactly as n is, so this becomes

$$\sum_{n \text{ even}} \left[q^{n^2} + q^{n^2} \right] + \sum_{n \text{ odd}} \left[q^{n^2} - q^{n^2} \right] = 2 \sum_{n \text{ even}} q^{n^2}$$

and finally a change of variable gives

$$2\sum_{n\text{ even}} q^{n^2} = 2\sum_{m=-\infty}^{\infty} q^{(2m)^2} = 2\sum_{m=-\infty}^{\infty} q^{4m^2} = 2\sum_{m=-\infty}^{\infty} (q^4)^{m^2} = 2\phi(q^4).$$

Showing (18) is slightly more fiddly; proceed as above to get to

$$\begin{aligned}\phi(q)-\phi(-q) &= 2\sum_{n\text{ odd}} q^{n^2} = 2\sum_{m=-\infty}^{\infty} q^{(2m+1)^2}\\ &= 2\sum_{m=-\infty}^{\infty} q^{4m^2+4m+1} = 2q\sum_{m=-\infty}^{\infty} (q^4)^{m(m+1)}\end{aligned}$$

As previously, an informal table suggests that the terms from $m \in \{0,1,2,\ldots\}$ are the same as those from $m \in \{-1,-2,-3,\ldots\}$, so splitting the sum, changing variables to $m = -(r+1)$ in the 'negative' one, and re-combining, gives

$$\phi(q)-\phi(-q) = 4q\sum_{m=0}^{\infty}(q^4)^{m(m+1)} = 4q\sum_{m=0}^{\infty}(q^8)^{m(m+1)/2} = 4q\psi(q^8).$$

Finally, to show (19), we work with the product forms, (10) and (11), and are required to show

$$\left[(-q;q^2)_\infty^2(q^2;q^2)_\infty\right]\left[(-q^2;q^4)_\infty(q^8;q^8)_\infty\right] = (-q;q^2)_\infty^2(q^4;q^4)_\infty^2.$$

This immediately is equivalent to

$$(q^2;q^2)_\infty(-q^2;q^4)_\infty(q^8;q^8)_\infty = (q^4;q^4)_\infty^2.$$

On the LHS, de-interleave $(q^2;q^2)_\infty$ into $(q^2;q^4)_\infty(q^4;q^4)_\infty$, and re-order:

$$\text{LHS} = (q^4;q^4)_\infty(q^2;q^4)_\infty(-q^2;q^4)_\infty(q^8;q^8)_\infty.$$

Combine $(q^2;q^4)_\infty(-q^2;q^4)_\infty$ into the difference of squares $(q^4;q^8)_\infty$:

$$\text{LHS} = (q^4;q^4)_\infty(q^4;q^8)_\infty(q^8;q^8)_\infty$$

and finally interleave $(q^4;q^8)_\infty(q^8;q^8)_\infty = (q^4;q^4)_\infty$.

10 Sums of four triangular numbers

We can now finally work towards an expression for $\psi^4(q)$, which will give us the main result $t_4(n) = \sigma(2n+1)$.

We will use the expressions already found for ϕ^2 and ϕ^4 as follows. Multiplying (17) by (18), and using (19), we find

$$\begin{aligned}\phi^2(q)-\phi^2(-q) &= 8q\phi(q^4)\psi(q^8)\\ &= 8q\psi^2(q^4). \qquad (20)\end{aligned}$$

Considering the power series (14) for $\phi^2(q)$ leads to:

$$\phi^2(q) + \phi^2(-q) = 2\phi^2(q^2). \tag{21}$$

Starting with (14), we see

$$\begin{aligned}
\phi^2(q) &= 1 + 4\sum_{n=1}^{\infty}\big(d_{1,4}(n) - d_{3,4}(n)\big)q^n; \\
\phi^2(-q) &= 1 + 4\sum_{n=1}^{\infty}\big(d_{1,4}(n) - d_{3,4}(n)\big)(-q)^n; \\
\phi^2(q) + \phi^2(-q) &= 2\left[1 + 4\sum_{\substack{n=2 \\ n \text{ even}}}^{\infty}\big(d_{1,4}(n) - d_{3,4}(n)\big)q^n\right] \\
&= 2\left[1 + 4\sum_{m=1}^{\infty}\big(d_{1,4}(2m) - d_{3,4}(2m)\big)(q^2)^m\right].
\end{aligned}$$

We now claim $d_{1,4}(2m) = d_{1,4}(m)$. Any factor of m is a factor of $2m$; we show that the 'extra' factors of $2m$ make no contribution to $d_{1,4}(2m)$.

Take a factor c of $2m$ which is not also a factor of m. Then $2m = ac$ for some a. Clearly $2 \mid ac$; we claim $2 \mid c$. Suppose not; then we must have $2 \mid a$, say $a = 2b$. But then $2m = (2b)c$, so $m = bc$, whereas our assumption was that $c \nmid m$. For this extra factor c, then, $c \in \{0, 2\} \pmod 4$, and c makes no contribution to $d_{1,4}(2m)$.

The same argument shows that $d_{3,4}(2m) = d_{3,4}(m)$, and we conclude that

$$\begin{aligned}
\phi^2(q) + \phi^2(-q) &= 2\left[1 + 4\sum_{m=1}^{\infty}\big(d_{1,4}(m) - d_{3,4}(m)\big)(q^2)^m\right] \\
&= 2\phi^2(q^2)
\end{aligned}$$

as required.

By multiplying (20) and (21), then using (19), we find

$$\phi^4(q) - \phi^4(-q) = 16q\psi^2(q^4)\phi^2(q^2) = 16q\psi^4(q^2)$$

and using the power series (16) for $\phi^4(q)$, we have

$$\text{LHS} = 8\sum_{m=0}^{\infty}\sum_{\substack{d|m\\4\nmid d}} dq^m - 8\sum_{m=0}^{\infty}\sum_{\substack{d|m\\4\nmid d}} d(-q)^m$$

$$= 16\sum_{\substack{m=1\\m \text{ odd}}}^{\infty}\sum_{\substack{d|m\\4\nmid d}} dq^m;$$

$$\text{RHS} = 16\sum_{n=0}^{\infty} t_4(n)q^{2n+1}.$$

Equating coefficients gives

$$t_4(n) = \sum_{\substack{d|(2n+1)\\4\nmid d}} d.$$

We finally note that '$4 \nmid d$' is superfluous for divisors d of the odd integer $2n+1$, and we have the result:

$$t_4(n) = \sigma(2n+1).$$

This completes the proof of (2), and hence also the explanation of `isToad`'s behaviour.

References

[1] Bruce C. Berndt. *Number Theory in the Spirit of Ramanujan*, volume 34 of *Student Mathematical Library*. American Mathematical Society, 2006.

[2] Peter J. Cameron. *Combinatorics: Topics, Techniques, Algorithms*. Cambridge University Press, 1994.

[3] Marc LeBrun. Computist quiz. `http://www.hackersdelight.org/quiz.pdf`, 2004.