Addition and Counting: The Arithmetic of Partitions

Scott Ahlgren and Ken Ono

At first glance the stuff of partitions seems like child's play:

$$4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1.$$

Therefore, there are 5 partitions of the number 4. But (as happens in number theory) the seemingly simple business of counting the ways to break a number into parts leads quickly to some difficult and beautiful problems. Partitions play important roles in such diverse areas of mathematics as combinatorics, Lie theory, representation theory, mathematical physics, and the theory of special functions, but we shall concentrate here on their role in number theory (for which [A] is the standard reference).

In the Beginning, There Was Euler...

A *partition* of the natural number n is any nonincreasing sequence of natural numbers whose sum is n (by convention, we agree that $p(0) = 1$). The number of partitions of n is denoted by $p(n)$. Eighty years ago Percy Alexander MacMahon, a major in the British Royal Artillery and a master calculator, computed the values of $p(n)$ for all n up to 200. He found that

$$p(200) = 3,972,999,029,388,$$

and he did not count the partitions one-by-one:

$$200 = 199+1 = 198+2$$
$$= 198+1+1 = 197+3 = \ldots\ldots\ldots\ldots\ldots .$$

Instead, MacMahon employed classical formal power series identities due to Euler.

To develop Euler's recurrence, we begin with the elementary fact that if $|x| < 1$, then

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \ldots .$$

Using this, Euler noticed that when we expand the infinite product

$$\prod_{n=1}^{\infty} \frac{1}{1-x^n} = (1 + x + x^2 + x^3 + \ldots)$$
$$\times (1 + x^2 + x^4 + \ldots)$$
$$\times (1 + x^3 + x^6 + \ldots)\ldots,$$

the coefficient of x^n is equal to $p(n)$ (think of the first factor as counting the number of 1's in a partition, the second as counting the number of 2's, and so on). In other words, we have the generating function

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1-x^n}$$
$$= 1 + x + 2x^2 + 3x^3 + 5x^4 + \ldots .$$

Moreover, Euler observed that the reciprocal of this infinite product satisfies a beautiful identity

Scott Ahlgren is assistant professor of mathematics at the University of Illinois, Urbana-Champaign. His e-mail address is ahlgren@math.uiuc.edu.

Ken Ono is professor of mathematics at the University of Wisconsin-Madison. His e-mail address is ono@math.wisc.edu.

Both authors thank the National Science Foundation for its support. The second author thanks the Alfred P. Sloan Foundation, the David and Lucile Packard Foundation, and the Number Theory Foundation for their support.

(also known as Euler's Pentagonal Number Theorem):

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{k=-\infty}^{\infty}(-1)^k x^{(3k^2+k)/2} = 1 - x - x^2 + x^5 + x^7 - x^{12} - \dots .$$

These two identities show that

$$\left(\sum_{n=0}^{\infty} p(n)x^n\right) \times \left(1 - x - x^2 + x^5 + x^7 - x^{12} - \dots\right) = 1,$$

which in turn implies, for positive integers n, that

$$p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + \dots .$$

This recurrence enabled MacMahon to perform his massive calculation.

Hardy-Ramanujan-Rademacher Asymptotic Formula for $p(n)$

It is natural to ask about the size of $p(n)$. The answer to this question is given by a remarkable asymptotic formula, discovered by G. H. Hardy and Ramanujan in 1917 and perfected by Hans Rademacher two decades later. This formula is so accurate that it can actually be used to compute individual values of $p(n)$; Hardy called it "one of the rare formulae which are both asymptotic and exact." It stands out further in importance since it marks the birth of the *circle method*, which has grown into one of the most powerful tools in analytic number theory.

Here we introduce Rademacher's result. He defined explicit functions $T_q(n)$ such that for all n we have

$$p(n) = \sum_{q=1}^{\infty} T_q(n).$$

The functions $T_q(n)$ are too complicated to write down here, but we mention that $T_1(n)$ alone yields the asymptotic formula

$$p(n) \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{2n/3}}.$$

(In their original work, Hardy and Ramanujan used slightly different functions in place of the $T_q(n)$. As a result, their analogue of the series $\sum_{q=1}^{\infty} T_q(n)$ was divergent, although still useful.) Moreover, Rademacher computed precisely the error incurred by truncating this series after Q terms. In particular, there exist explicit constants A and B such that

$$\left| p(n) - \sum_{q=1}^{A\sqrt{n}} T_q(n) \right| < \frac{B}{n^{1/4}}.$$

Since $p(n)$ is an integer, this determines the exact value of $p(n)$ for large n. The rate at which Rademacher's series converges is remarkable; for example, the first eight terms give the approximation

$$p(200) \approx 3,972,999,029,388.004$$

(compare with the exact value computed by MacMahon).

To implement the circle method requires a detailed study of the analytic behavior of the generating function for $p(n)$. Recall that we have

$$F(x) := \sum_{n=0}^{\infty} p(n)x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)\dots}.$$

This is an analytic function on the domain $|x| < 1$. A natural starting point is Cauchy's Theorem, which gives

$$p(n) = \frac{1}{2\pi i}\int_C \frac{F(x)}{x^{n+1}}\,dx,$$

where C is any simple closed counterclockwise contour around the origin. One would hope to adjust the contour in relation to the singularities of $F(x)$ in order to obtain as much information as possible about the integral. But consider for a moment these singularities; they occur at *every* root of unity, forming an impenetrable barrier on the unit circle. In our favor, however, it can be shown that the size of $F(x)$ near a primitive q-th root of unity diminishes rapidly as q increases; moreover the behavior of $F(x)$ near each root of unity can be described with precision. Indeed, with an appropriate choice of C, the contribution to the integral from all of the primitive q-th roots of unity can be calculated quite precisely. The main contribution is the function $T_q(n)$; a detailed analysis of the errors involved yields the complete formula.

The circle method has been of extraordinary importance over the last eighty years. It has played a fundamental role in additive number theory (in Waring type problems, for instance), analysis, and even the computation of black hole entropies.

Ramanujan's Congruences

After a moment's reflection on the combinatorial definition of the partition function, we have no particular reason to believe that it possesses any interesting arithmetic properties (the analytic formula of the last section certainly does nothing to change this opinion). There is nothing, for example, which would lead us to think that $p(n)$ should exhibit a preference to be even rather than odd. A natural suspicion, therefore, might be that the values of $p(n)$ are distributed evenly modulo 2. A quick computation of the first 10,000 values confirms this suspicion: of these 10,000 values, exactly 4,996 are even and 5,004 are odd. This pattern continues with 2 replaced by 3: of the first 10,000 values, 3,313; 3,325; and 3,362 (in each case almost exactly


Euler

one-third) are congruent respectively to 0, 1, and 2 modulo 3. When we replace 3 by 5, however, something quite different happens: we discover that 3,611 (many more than the expected one-fifth) of the first 10,000 values of $p(n)$ are divisible by 5. What is the explanation for this aberration?

The answer must have been clear to Ramanujan when he saw MacMahon's table of values of $p(n)$. So Ramanujan would have seen something like the following.

1	1	2	3	5
7	11	15	22	30
42	56	77	101	135
176	231	297	385	490
627	792	1002	1255	1575
1958	2436	3010	3718	4565

What is striking, of course, is that every entry in the last column is a multiple of 5. This phenomenon, which persists, explains the apparent aberration above and was the first of Ramanujan's ground-breaking discoveries on the arithmetic of $p(n)$. Here is his own account.

> *I have proved a number of arithmetic properties of $p(n)$…in particular that*
>
> $$p(5n+4) \equiv 0 \pmod 5,$$
> $$p(7n+5) \equiv 0 \pmod 7.$$
>
> *…I have since found another method which enables me to prove all of these properties and a variety of others, of which the most striking is*
>
> $$p(11n+6) \equiv 0 \pmod{11}.$$
>
> *There are corresponding properties in which the moduli are powers of 5, 7, or 11…. It appears that there are no equally simple properties for any moduli involving primes other than these three.*

Ramanujan proved these congruences in a series of papers (the proofs of the congruences modulo 5 and 7 are quite ingenious but are not terribly difficult, while the proof of the congruence modulo 11 is much harder). In these same papers he sketched proofs of extensions of these congruences. For example, we have

$$p(25n+24) \equiv 0 \pmod{25},$$
$$p(49n+47) \equiv 0 \pmod{49}.$$

Ramanujan noticed the beginnings of other patterns in these first 200 values:

$$p(116) \equiv 0 \pmod{121}, \quad p(99) \equiv 0 \pmod{125}.$$

From such scant evidence he made the following conjecture:

$$\textit{If } \delta = 5^a 7^b 11^c \textit{ and } 24\lambda \equiv 1 \pmod{\delta},$$
$$\textit{then } p(\delta n + \lambda) \equiv 0 \pmod{\delta}.$$

When $\delta = 125$, for example, we have $\lambda = 99$. So Ramanujan's conjecture is that

$$p(125n+99) \equiv 0 \pmod{125}.$$

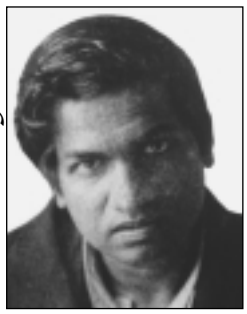
We note that the general conjecture follows easily from the cases when the moduli are powers of 5, 7, or 11.

It is remarkable that Ramanujan was able to formulate a general conjecture based on such little evidence and therefore unsurprising that the conjecture was not quite correct (in the 1930s Chowla and Gupta discovered the counterexample $p(243) \not\equiv 0 \pmod{7^3}$). Much to Ramanujan's credit, however, a slightly modified version of his conjecture is indeed true; in particular, we now know the following:

$$\textit{If } \delta = 5^a 7^b 11^c \textit{ and } 24\lambda \equiv 1 \pmod{\delta},$$
$$\textit{then } p(\delta n + \lambda) \equiv 0 \pmod{5^a 7^{\lfloor \frac{b}{2} \rfloor + 1} 11^c}.$$

The task of assigning credit for the proofs of these conjectures when the modulus is a power of 5 or 7 poses an interesting historical challenge. Typically, the proofs have been attributed to G. N. Watson. Recently, however, the nature of Ramanujan's own contributions [R] has been greatly clarified. Indeed, a complete outline of the proof modulo powers of 5 and a much rougher sketch for powers of 7 (so rough that it did not yet reveal his error in the statement of the conjecture) are given by Ramanujan in a long manuscript which he wrote in the three years preceding his

Hardy 

Ramanujan 

Rademacher 

death. In typical fashion, Ramanujan provides in neither case complete details for all of his assertions. This manuscript was apparently in Watson's possession from 1928 until his death in 1965. Indeed, a copy of the manuscript in Watson's handwriting (the whereabouts of the original is unknown) resides in the library of Oxford's Mathematical Institute. In any event, it seems clear that Ramanujan deserves more credit than he has historically been granted for these cases. By contrast, the case of powers of 11 is much more difficult; the first published proof of Ramanujan's conjectures in this case was given by A. O. L. Atkin in 1967.

Dyson's Rank and Crank

The celebrated physicist Freeman Dyson, when he was a college student in 1944, initiated an important subject in partition theory by discovering a delightfully simple phenomenon which appeared to explain why

$$p(5n+4) \equiv 0 \pmod 5$$

and

$$p(7n+5) \equiv 0 \pmod 7.$$

Dyson defined the *rank* of a partition to be the largest summand minus the number of summands. Here, for example, are the partitions of 4 and their ranks:

Partition	Rank
4	$4-1 \equiv 3 \pmod 5$,
$3+1$	$3-2 \equiv 1 \pmod 5$,
$2+2$	$2-2 \equiv 0 \pmod 5$,
$2+1+1$	$2-3 \equiv 4 \pmod 5$,
$1+1+1+1$	$1-4 \equiv 2 \pmod 5$.

Notice that the ranks of these partitions represent each residue class modulo 5 exactly once. After computing many more examples, Dyson observed that, without exception, numbers of the form $5n+4$ (respectively $7n+5$) have the property that their ranks modulo 5 (respectively modulo 7) are equally distributed. More precisely, if $0 \le m < M$ are integers and $R(N,m,M)$ denotes the number of partitions of N with rank congruent to $m \pmod M$, then Dyson conjectured that

$$R(5n+4,m,5) = \frac{1}{5} \cdot p(5n+4) \quad \text{for } 0 \le m \le 4,$$

$$R(7n+5,m,7) = \frac{1}{7} \cdot p(7n+5) \quad \text{for } 0 \le m \le 6.$$

The truth of these conjectures would provide a simple and elegant combinatorial explanation for Ramanujan's congruences. Dyson's speculation was confirmed ten years later by Atkin and H. P. F. Swinnerton-Dyer in a wonderful paper which combines classical combinatorial arguments with techniques from the theory of modular functions.

Unfortunately, Dyson's rank does not seem to enjoy such simple properties for primes other than 5 and 7. However, he conjectured the existence of another natural statistic, the *crank*, which explains the congruence

$$p(11n+6) \equiv 0 \pmod{11}.$$

In the late 1980s George E. Andrews and Frank Garvan found such a crank [A-G], [G]. Further work of Garvan, Dongsu Kim, and Dennis Stanton [G-K-S] has produced, for the congruences with moduli 5, 7, 11, and 25, combinatorial interpretations which are rooted in the modular representation theory of the symmetric group.

Atkin's Examples

We return to Ramanujan's intuition that there are no simple arithmetic properties for $p(n)$ when the modulus involves primes greater than 11. Ramanujan seems to have been correct in this claim; no new congruence as simple as the originals has ever been found (although it has not been proved that none exists). The 1960s, however, witnessed tantalizing discoveries of further examples (notably by Atkin, Newman, and O'Brien). Atkin, for example, found elegant infinite families of congruences modulo 5, 7, and 13 which are quite different from those previously known. A simple example of these is the congruence

$$p(11^3 \cdot 13n + 237) \equiv 0 \pmod{13}.$$

Atkin also gave more examples, though not so systematic, with moduli 17, 19, 23, 29, and 31.

Atkin obtains these results via a detailed study of modular functions. Since these lie at the heart of the proofs of the congruences we have

seen so far, we will give a brief description here. Let $\mathrm{SL}_2(\mathbb{Z})$ be the set of 2×2 integer matrices with determinant equal to 1. Then, if N is an integer, define the *congruence subgroup* $\Gamma_0(N)$ by

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

An element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on the upper half-plane $\mathbb{H}$ of complex numbers via the linear fractional transformation $\gamma z = \frac{az+b}{cz+d}$. By definition, a *modular function* on $\Gamma_0(N)$ is a function f on $\mathbb{H}$ which satisfies $f(\gamma z) = f(z)$ for all $\gamma \in \Gamma_0(N)$ and which in addition is meromorphic on $\mathbb{H}$ and "at the cusps". When N is small, the field of these functions is relatively simple; therefore, given several functions in such a field, one expects to find nontrivial relations among them. If the right functions are involved, then such a relation may give information about values of $p(n)$. For Atkin's examples when $\ell = 5$, 7, or 13, the relevant function fields have a single generator; this is responsible for the infinite families of congruences. As ℓ increases, however, things rapidly become more complicated. Atkin's work is interesting for another reason: it marks an early use of sophisticated computers in mathematics. As he says, "It is often more difficult to discover results in this subject than to prove them, and an informed search on the machine may enable one to find out precisely what happens."

A Problem of Erdős

Even after all of the beautiful discoveries described above, the general arithmetic properties of $p(n)$ must seem rather mysterious. Indeed, we have said nothing for any prime modulus ℓ greater than 31, let alone for a general prime modulus. In this context we mention a conjecture of Erdős from the 1980s.

If ℓ is a prime, then there exists an n such that $p(n) \equiv 0 \pmod{\ell}$.

If we reflect on this conjecture for a moment, we are struck by its weakness: it asserts only that every prime divides at least *one* value of the partition function. On the other hand, (until very recently) the known results were even weaker; the best was a theorem of Schinzel and Wirsing, who proved the existence of a constant c such that, for large X, the number of primes $\ell < X$ for which Erdős's conjecture is true is $\geq c \log\log X$.

Recent Developments

In the past several years our understanding of the arithmetic of $p(n)$ has increased dramatically. All of the advances have arisen from a single source: the fact that values of the partition function are intimately related to the arithmetic of modular forms. Modular forms have historically played a large role in number theory; their importance, of course, has been underscored by their central position in the proof of Fermat's Last Theorem. The crux of Wiles' proof is to show that elliptic curves are "modular"; in other words, their arithmetic is dictated in part by certain modular forms to which they are related. What has been learned recently is that the partition function does not escape the web of modularity; its arithmetic, too, is intimately connected to the behavior of a certain family of modular forms. This connection has allowed the application of deep methods of Deligne, Serre, and Shimura to the study of $p(n)$. These theories (some of the most powerful of the last half-century) have important ramifications for $p(n)$; in particular, properly applied, they imply that $p(n)$ satisfies linear congruences for *every* prime $\ell \geq 5$. We shall discuss in more detail how modular forms enter the picture in the next section; let us first indicate what they enable us to prove.

The second author (inspired by some formulae of Ramanujan) was the first to notice these connections; as a result [O] he proved the following:

For any prime $\ell \geq 5$, there exist infinitely many congruences of the form

$$p(An + B) \equiv 0 \pmod{\ell}.$$

(We note that if the arithmetic progression $An + B$ gives rise to such a congruence, then so do any of its infinitely many subprogressions; we do not count these as new when we speak of "infinitely many congruences".) Shortly thereafter the first author [Ahl] extended this result by showing that the prime ℓ may in fact be replaced by an arbitrary prime power ℓ^k; from this it can be shown that ℓ may in fact be replaced by any modulus M which is coprime to 6. An immediate consequence of these results is the following:

If $\ell \geq 5$ is prime, then a positive proportion of natural numbers n have $p(n) \equiv 0 \pmod{\ell}$.

This provides a very convincing proof of the conjecture of Erdős mentioned above.

More recently, the two authors [Ahl-O] have shown that congruences for $p(n)$ are even more widespread than these theorems indicate. To explain this, let us return to Ramanujan's original results:

$$p(5n + 4) \equiv 0 \pmod{5},$$
$$p(7n + 5) \equiv 0 \pmod{7},$$
$$p(11n + 6) \equiv 0 \pmod{11}.$$

As Ramanujan's conjectures indicate, these results may be written in a unified way. Namely, let λ_ℓ denote the inverse of 24 modulo ℓ (in other words, $24\lambda_\ell \equiv 1 \pmod{\ell}$). Then they assume the following form:

If $\ell = 5, 7, or\ 11$, *then* $p(\ell n + \lambda_\ell) \equiv 0 \pmod{\ell}$.

Now, for any prime $\ell \geq 5$ and any exponent k, the results above guarantee the existence of infinitely many progressions $An + B$ such that $p(An + B) \equiv 0 \pmod{\ell^k}$. An important feature of the method used to prove the theorems above is that in every case, the progression $An + B$ which it produces is a subprogression of $\ell n + \lambda_\ell$ (in other words, $\ell \mid A$ and $B \equiv \lambda_\ell \pmod{\ell}$). As an example, one of the simplest congruences guaranteed by this theorem is

$$p(59^4 \cdot 13n + 111247) \equiv 0 \pmod{13};$$

in this case we have $111247 \equiv 1/24 \pmod{13}$.

What the authors have shown recently is that congruences are not confined to this single progression modulo ℓ. In fact, we now know that if $\ell \geq 5$ is prime and k is any exponent, then infinitely many congruences $p(An + B) \equiv 0 \pmod{\ell^k}$ exist within each of $(\ell + 1)/2$ progressions modulo ℓ. In other words, for each prime, slightly more than half of such progressions contain congruences. When $\ell = 11$, for example, the relevant progressions are

$$11n + 1,\ 11n + 2,\ 11n + 3,$$
$$11n + 5,\ 11n + 6,\ 11n + 8.$$

Of these, only Ramanujan's own $11n + 6$ had been distinguished by the previous theory. The latest result provides a theoretical framework which explains every known partition function congruence.

Modular Forms

We will try to indicate briefly how the theory of modular forms can be applied to the study of $p(n)$ in order to yield the results of the preceding section. At the heart of the matter are the generating function

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1 - x^n}$$

and Dedekind's eta function

$$\eta(z) = x^{1/24} \prod_{n=1}^{\infty} (1 - x^n) \quad (\text{here } x := e^{2\pi i z}).$$

Combining the last two formulae gives

$$1/\eta(24z) = \sum_{n=-1}^{\infty} p\left(\frac{n+1}{24}\right) x^n = x^{-1} + x^{23} + \dots .$$

Loosely speaking, a *modular form* of weight k on the subgroup $\Gamma_0(N)$ is a function f on the upper half-plane $\mathbb{H}$ which satisfies a transformation property of the form

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z) \quad \text{for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N).$$

In addition, f is required to be meromorphic on $\mathbb{H}$ and at the cusps; if f is also holomorphic on $\mathbb{H}$ and vanishes at the cusps, then we call f a *cusp form*. We allow k to be an integer or half an integer (extra care must be taken in the latter case); note that the modular functions introduced above are just modular forms of weight zero. Every modular form $f(z)$ has a Fourier expansion in powers of $x = e^{2\pi i z}$; if f is a cusp form, then this expansion takes the form

$$f(z) = \sum_{n=1}^{\infty} a_f(n) x^n.$$

When the weight k of a cusp form is integral, then the theory of Deligne and Serre is available for the study of the Fourier coefficients a_f. In particular, there is a natural family of operators (the so-called Hecke operators) that act on spaces of modular forms. If f is a normalized eigenform for this family, then Serre conjectured and Deligne proved the existence of a representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$$

(for some field K) such that for all but finitely many primes Q we have

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_Q)) = a_f(Q).$$

Here Frob_Q denotes a Frobenius element at the prime Q. This result is extraordinarily powerful; it allows us to study the Fourier coefficients of modular forms using the structure of Galois groups.

If the weight k of a cusp form is half-integral, then we do not have the results of Deligne and Serre at our disposal. There is, however, a correspondence due to Shimura between cusp forms of half integral weight and certain forms of integral weight; the Shimura correspondence is quite explicit and commutes in the best possible way with the action of the Hecke operators on the respective spaces.

We saw above that the expansion

$$1/\eta(24z) = \sum_{n=-1}^{\infty} p\left(\frac{n+1}{24}\right) x^n = x^{-1} + x^{23} + \dots$$

contains every value of the partition function. Now $1/\eta(24z)$ is a modular form on $\Gamma_0(576)$. However, it has two major deficiencies: the weight is $-1/2$, and it has a pole at every cusp. So none of the theories above seem to apply. It turns out, however, that starting with this expansion, one can construct half-integral weight cusp forms which still preserve much information about the values of $p(n)$ modulo powers of primes. From these cusp forms the theory of Deligne and Serre, filtered through Shimura's correspondence, yields the results of the preceding section.

L-Functions and Arithmetic

Since modular forms play such an important role in partition congruences, it is natural to suspect

that there may be deeper connections between partitions and "modular" objects. As it turns out, this is indeed the case.

To motivate the connection, consider the following classical Diophantine question (already of interest to ancient Greek and Arab scholars):

Which integers D are areas of right triangles with rational number sidelengths?

Such numbers D are known as *congruent numbers*. Simple arguments show that a number D is congruent precisely when there are infinitely many rational points (x, y) on the elliptic curve

$$E_D : y^2 = x^3 - D^2 x.$$

How does one determine whether such a curve has infinitely many points? The Birch and Swinnerton-Dyer Conjecture, one of the main outstanding conjectures in number theory (and a million-dollar Clay Mathematics Institute problem), provides the solution.

Let $L(E_D, s)$ denote the Hasse-Weil L-function attached to E_D; this is an analytic function whose definition depends on the behavior of E_D modulo primes p. For the congruent number problem the conjecture implies that

$$L(E_D, 1) = 0 \iff D \text{ is congruent.}$$

In addition, the conjecture gives a precise formula dictating the analytic behavior of $L(E_D, s)$ at $s = 1$. For instance, if $L(E_D, 1) \neq 0$, then the conjecture asserts that

$$L(E_D, 1) = \Omega_D \cdot \#Ш(E_D).$$

Here Ω_D is an explicit transcendental number, and $Ш(E_D)$ is the Tate-Shafarevich group of E_D. (The Tate-Shafarevich group is a certain Galois cohomology group which measures the extent to which the local-global principle fails for E_D.)

In the early 1980s Jerrold Tunnell, using the works of Shimura and Waldspurger (see [K] for a good account), constructed two modular forms of weight 3/2 whose coefficients "interpolate" the square roots of the $L(E_D, 1)$. Together with the Birch and Swinnerton-Dyer Conjecture, these modular forms provide a complete solution to the congruent number problem.

Recently, Li Guo and the second author [G-O] have shown that if $13 \leq \ell \leq 31$ is prime, then certain half-integral weight modular forms whose coefficients interpolate values of $p(n)$ modulo ℓ behave in a manner somewhat similar to Tunnell's modular forms. In particular, they showed that there are *modular motives* $M_{D,\ell}$ (these may be viewed as analogs of elliptic curves) whose L-functions $L(M_{D,\ell}, s)$ have the property that the square roots of $L(M_{D,\ell}, (\ell - 3)/2)$ are related in a predictable way to the coefficients of these modular forms. The truth of the Bloch-Kato Conjecture (a vast generalization of the Birch and Swinnerton-Dyer Conjecture) then implies that

$$L(M_{D,\ell}, (\ell - 3)/2) = \Omega_{D,\ell} \cdot \#Ш(M_{D,\ell}).$$

Assuming the Bloch-Kato Conjecture, it can be shown, for many n, that

$$p(n) \equiv 0 \pmod{\ell} \implies \#Ш(M_{D,\ell}) \equiv 0 \pmod{\ell},$$

where D depends on n. These two conditions are probably equivalent, and so it is likely that the divisibility of $p(n)$ often dictates the presence of elements of order ℓ in these Tate-Shafarevich groups. So, perhaps surprisingly, it seems that congruences like Ramanujan's are connected to some highly abstract creations of modern number theory.

The Future?

The beginnings of the partition function are extraordinarily humble; after all, what could be simpler than addition and counting? Despite its humble start, the history of the partition function includes connections to many central areas of number theory, from the work of Euler to the birth of the circle method to the modern theory of modular forms and L-functions. It will be quite interesting to see what further connections the future will reveal.

References

[Ahl] S. Ahlgren, The partition function modulo composite integers M, *Math. Ann.* **318** (2000), 795–803.

[Ahl-O] S. Ahlgren and K. Ono, Congruence properties for the partition function, *Proc. Nat. Acad. Sci. U.S.A.*, to appear.

[A] G. E. Andrews, *The Theory of Partitions*, Cambridge Univ. Press, 1998.

[A-G] G. E. Andrews and F. Garvan, Dyson's crank of a partition, *Bull. Amer. Math. Soc. (N.S.)* **18** (1988), 167–171.

[R] B. C. Berndt and K. Ono, Ramanujan's unpublished manuscript on the partition and tau functions with commentary, *The Andrews Festschrift* (D. Foata and G. N. Han, eds.), Springer-Verlag, 2001, pp. 39–110.

[G] F. Garvan, New combinatorial interpretations of Ramanujan's partition congruences mod 5, 7 and 11, *Trans. Amer. Math. Soc.* **305** (1988), 47–77.

[G-K-S] F. Garvan, D. Kim, and D. Stanton, Cranks and t-cores, *Invent. Math.* **101** (1990), 1–17.

[G-O] L. Guo and K. Ono, The partition function and the arithmetic of certain modular L-functions, *Internat. Math. Res. Notices* **21** (1999), 1179–1197.

[K] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1993.

[O] K. Ono, Distribution of the partition function modulo m, *Ann. of Math.* **151** (2000), 293–307.

Note: Photograph of L. Euler courtesy of the Institut Mittag-Leffler. The photograph of H. Rademacher was provided by Bruce Berndt.