RAMANUJAN, TAXICABS, BIRTHDATES, ZIPCODES, AND TWISTS

Ken Ono

American Mathematical Monthly, 104, No. 10, 1997, pages 912-917.

It is well known that G. H. Hardy travelled in a taxicab numbered 1729 to an English nursing home to visit his bedridden colleague S. Ramanujan. Hardy was disappointed that his cab had such a mundane number, but to his surprise when he mentioned this to Ramanujan, the brilliant Indian mathematician found 1729 to be quite interesting, for it is the smallest integer that has two distinct representations as a sum of two cubes:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

J. H. Silverman used this famous anecdote to motivate the study of elliptic curves in a recent article [8].

Recently I learned that other permutations of the digits 1, 2, 7, and 9 are significant to the Ramanujan story. Two permutations involve Bruce Berndt, the diligent editor of Ramanujan's notebooks. Bruce has devoted most of his professional career to undertaking the daunting task of proving many of Ramanujan's identities (written in notebooks without proofs), but to my surprise his fascination with Ramanujan has profoundly impacted his life outside mathematics. Sonja, Bruce's youngest daughter, was born in 1972. Is this a coincidence, or could it be an example of "Ramanujan family planning?" With more sleuthing I discovered that Bruce's home is in Urbana, Illinois 61802-**7219**. Could there be any truth to the rumor that Bruce paid the postmaster a mere $12.79 for this vanity zipcode?

In a more serious direction, consider the number 2719, which came to my attention in joint work with K. Soundararajan [5]. We begin with the following footnote from Ramanujan's 1916 paper on quadratic forms [6, p. 14]:

"... *the even numbers which are not of the form* $x^2 + y^2 + 10z^2$ *are the numbers*

$$4^\lambda(16\mu + 6),$$

while the odd numbers that are not of that form, viz.,

$$3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391 \dots$$

do not seem to obey any simple law."

Typeset by $\mathcal{AMS}$-TeX

In view of the list of exceptions, could there be a "simple law" that eluded Ramanujan? After extensive computation, amongst the odd integers two further exceptions emerged, the numbers 679 and of course 2719. A few years ago W. Duke and R. Schulze-Pillot [3] (see [2] for a survey) made a great breakthrough in the theory of ternary quadratic forms, and from their work it follows that there are only finitely many positive odd integers that are not of the form $x^2 + y^2 + 10z^2$. Could it be that 2719 is the largest such integer?

Unfortunately we do not yet know enough to decide whether or not it is since they obtained no bound beyond which every odd integer is so represented. Although obtaining such a bound appears to be beyond the current state of knowledge, assuming certain Riemann hypotheses, the author and Soundararajan [5] have shown that the only positive odd integers that are not of the form $x^2 + y^2 + 10z^2$ are indeed 679, 2719, and the 16 numbers on Ramanujan's list. Therefore we have very good reason to believe that 2719 is the largest odd integer that is not of the form $x^2 + y^2 + 10z^2$.

Here we explore the special properties that these eighteen integers share. Obviously they are odd numbers n for which there are no integers x, y, and z with $n = x^2 + y^2 + 10z^2$, and we even know that they are all square-free (see [1], [5,Th. 1]) and coprime to 10, but these numbers are linked for much deeper reasons involving some of the most fundamental objects in algebraic number theory and arithmetic geometry. Let me explain.

Following C. F. Gauss, any collection of equivalence classes of ternary quadratic forms that represent the same residue classes $\pmod{M}$ for every M is called a "genus." In our case, the genus containing Ramanujan's ternary quadratic form $x^2 + y^2 + 10z^2$ contains only one other class, and a representative for this class is the form $2x^2 + 2y^2 + 3z^2 - 2xz$. For convenience define $r_1(n)$ and $r_2(n)$ by

$$
\begin{aligned}
r_1(n) &:= \#\{(x, y, z) \mid x, y, z \in \mathbb{Z},\ x^2 + y^2 + 10z^2 = n\},\\
r_2(n) &:= \#\{(x, y, z) \mid x, y, z \in \mathbb{Z},\ 2x^2 + 2y^2 + 3z^2 - 2xz = n\}.
\end{aligned}
$$

Therefore, Ramanujan wanted a rule for determining those odd n for which $r_1(n) = 0$.

To see the utility in considering both forms together recall Gauss' Three Squares Theorem. Let $h(D)$ denote the number of classes of primitive binary quadratic forms with discriminant D, the usual "class number," and let $r(n)$ denote the number of representations of n by $x^2 + y^2 + z^2$. If $n > 3$ is square-free, then

$$
r(n) = \begin{cases} 12h(-4n) & \text{if } n \equiv 1, 2, 5, 6 \pmod{8},\\ 24h(-n) & \text{if } n \equiv 3 \pmod{8}. \end{cases}
$$

More generally, Gauss obtained formulas for the number of representations of integers by genera, and in the case of Ramanujan's form, if n is a positive square-free integer coprime to 10, then

$$r_1(n)/2 + r_2(n) = h(-40n).$$

Therefore if n is a positive odd integer that is not of the form $x^2 + y^2 + 10z^2$, then

$$r_2(n) = h(-40n). \tag{1}$$

It is also useful to consider the differences $r_1(n) - r_2(n)$. To do so, define

(2)

$$f(z) := \frac{1}{4}\sum_{n=1}^{\infty}(r_1(n)-r_2(n))q^n = q - q^3 - q^7 - q^9 + 2q^{13} + \cdots \quad (q := e^{2\pi iz} \text{ with } Im(z) > 0).$$

This function f is a "weight 3/2 modular form." An analytic function $m(z)$ on the upper half of the complex plane is a modular form of weight k if for each suitable matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ there exist roots of unity $\epsilon(d)$ for which

$$m\left(\frac{az+b}{cz+d}\right) = \epsilon(d)(cz+d)^k m(z).$$

To study $r_1(n) - r_2(n)$ we employ the *Shimura lift* [7], a beautiful correspondence between certain half-integral weight modular forms and integral weight modular forms. In this case if integers $A(n)$ are defined by

$$\sum_{n=1}^{\infty}\frac{A(n)}{n^s} := \frac{1}{4}\cdot\left(\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}\right)\cdot\left(\sum_{m=1}^{\infty}\frac{r_1(m^2)-r_2(m^2)}{m^s}\right)$$

where χ denotes the Legendre-Kronecker quadratic character $\chi(n) := \left(\frac{-10}{n}\right)$, and if q and z are as in (2), then

$$(3)\quad F(z) := \sum_{n=1}^{\infty} A(n)q^n = q\prod_{n=1}^{\infty}(1-q^{2n})^2(1-q^{10n})^2 = q - 2q^3 - q^5 + 2q^7 + q^9 + 2q^{13} + \cdots$$

is a weight 2 modular form.

The modular form $F(z)$ provides an example of the celebrated Shimura-Taniyama Conjecture, whose proof in special cases by A. Wiles yields Fermat's Last Theorem. The conjecture asserts that the coefficients of certain weight 2 modular forms, the $A(n)$, equal the coefficients of L-functions of elliptic curves. In this case let E denote the elliptic curve over the rational numbers

$$E: \quad y^2 = x^3 + x^2 + 4x + 4.$$

For each odd prime p let $N(p)$ denote the number of pairs, $x \pmod{p}, y \pmod{p}$, that satisfy the congruence

$$y^2 \equiv x^3 + x^2 + 4x + 4 \pmod{p}.$$

If $c(p) := p - N(p)$, then the Hasse-Weil L-function $L(E,s)$ is defined by the following product over all the odd primes:

$$(4)\quad L(E,s) := \sum_{n=1}^{\infty}\frac{c(n)}{n^s} = \prod_{p\neq 2}\frac{1}{1-c(p)p^{-s}+p^{1-2s}} = 1 - \frac{2}{3^s} - \frac{1}{5^s} + \frac{2}{7^s} + \frac{1}{9^s} + \frac{2}{13^s} + \cdots.$$

By comparing (3) and (4) one sees that $A(n) = c(n)$ for each $n \le 13$. In fact this equality holds for every positive integer n, and is an example of the phenomenon described by the Shimura-Taniyama Conjecture.

Are these observations relevant to Ramanujan's query? They are, and the answer lies in the work of J.-L. Waldspurger [10] who provided a very deep and beautiful interpretation of Shimura's lift. In our case let n be a positive odd square-free integer, and define the $-10n$ quadratic twist $L(E(-10n), s)$ by

$$L(E(-10n), s) := \prod_{p \neq 2,5} \frac{1}{1 - c(p)\left(\frac{-10n}{p}\right)p^{-s} + p^{1-2s}}.$$

This is the L-function for the elliptic curve $E(-10n)$

$$E(-10n): \quad y^2 = x^3 - 10nx^2 + 400n^2x - 4000n^3.$$

If

$$\Omega := \int_{10}^{\infty} \frac{1}{\sqrt{x^3 - 10x^2 + 400x - 4000}} dx \sim 0.7195\ldots,$$

then for every odd square-free integer $n \neq 5$ Waldspurger's theorem implies

$$(r_1(n) - r_2(n))^2 = \frac{4\sqrt{n}}{\Omega} \cdot L(E(-10n), 1).$$

Therefore, by (1), if n is a positive odd integer that is not of the form $x^2 + y^2 + 10z^2$, then

$$h^2(-40n) = \frac{4\sqrt{n}}{\Omega} \cdot L(E(-10n), 1). \tag{5}$$

Although (5) is a "law" that the odd integers not of the form $x^2 + y^2 + 10z^2$ obey, it certainly is not a simple one. However, its formulation is particularly intriguing.

First we recall some facts about elliptic curves. Let C denote the set of rational points (x, y) satisfying

$$C: \qquad y^2 = x^3 + ax^2 + bx + c$$

where a, b and c are fixed rational numbers. If the discriminant of $x^3 + ax^2 + bx + c$ is non-zero, then Mordell proved that C, including a "point at infinity," forms a finitely generated abelian group whose group law is a "chord-tangent" law (see [9]). Therefore,

$$C \cong C_{\text{torsion}} \times \mathbb{Z}^r$$

where C_{torsion}, the torsion subgroup of C, is a finite abelian group, and the rank r is a non-negative integer. Note that C has finitely many points if and only if $r = 0$. Quite a bit is known about C_{torsion}. By a theorem of Mazur it is known that C_{torsion} satisfies

$$C_{\text{torsion}} \in \begin{cases} \mathbb{Z}m & | \text{ where } 1 \le m \le 10, \quad \text{or } m = 12, \\ \mathbb{Z}2 \times \mathbb{Z}2m & | \text{ where } 1 \le m \le 4 \end{cases}$$

($\mathbb{Z}d$ denotes the cyclic group with d elements), and with this classification it is fairly easy to deduce C_{torsion} for any given C.

Computing r is a more difficult question, and although one can typically compute r in practice, the problem in general remains open. In part these problems revolve around the Birch and Swinnerton-Dyer Conjecture, which asserts that the analytic behavior of $L(C,s)$ at $s=1$ predicts the structure of C, in particular r. In its weakest form the conjecture asserts that $L(C,s)$ has an analytic continuation to the entire complex plane, and that r equals the order of vanishing at $s=1$ of $L(C,s)$. In particular, C has finitely many points precisely when $L(C,1)\neq 0$.

For a "modular" elliptic curve C, one satisfying the Shimura-Taniyama Conjecture, V. Kolyvagin [4] proved that C has finitely many points if $L(C,1)\neq 0$. Therefore by the positivity of $h(-40n)$, (5), and Kolyvagin's theorem, if n is a positive odd integer that is not of the form $x^2+y^2+10z^2$, then $E(-10n)$ has finitely many points. In fact if n equals 679, 2719, or any of the 16 numbers on Ramanujan's list, then the only rational point (x,y) on $E(-10n)$

$$y^2 = x^3 - 10nx^2 + 400n^2x - 4000n^3,$$

is $(10n,0)$.

In its full strength the Birch and Swinnerton-Dyer Conjecture predicts even more. If $L(C,1)\neq 0$ the conjecture predicts that $L(C,1)$ is an explicit real multiple of the order of $Ш(C)$, the Tate-Shafarevich group of C, which measures the extent to which the "local-global principle" fails for an elliptic curve C. Recall that a conic has a point with rational coordinates precisely when it contains a point with real coordinates and a point with coordinates that are p-adic numbers for every prime p. However this is not true for elliptic curves. In a famous example, E. Selmer noted that there are no non-trivial rational points on

$$3x^3+4y^3+5z^3=0,$$

even though it has points over every field of p-adic numbers. The Tate-Shafarevich group measures the failure of this principle.

In our case if n is 679, 2719, or one of the 16 integers on Ramanujan's list, then (5) and the Birch and Swinnerton-Dyer Conjecture imply

$$h^2(-40n) = 4^{t(n)+1}\cdot |Ш(E(-10n))| \tag{6}$$

where $t(n)$ denotes the number of prime factors of n.

Just as Tate-Shafarevich groups measure the obstruction to the "local-global" principle for elliptic curves, the set of classes of discriminant D primitive binary quadratic forms, denoted by $CL(D)$, measures an obstruction. The set $CL(D)$ is an abelian group with order $h(D)$ that is isomorphic to the "ideal class group" of $\mathbb{Q}(\sqrt{D})$, and it measures the extent to which unique factorization fails in the ring of integers of $\mathbb{Q}(\sqrt{D})$. For instance, in the ring of integers of $\mathbb{Q}(\sqrt{-40})$, numbers of the form $a+b\sqrt{-10}$ with $a,b\in\mathbb{Z}$, the integer 14 does not factor uniquely into irreducibles since it has the following factorizations:

$$14 = 2\cdot 7 = (2+\sqrt{-10})\cdot(2-\sqrt{-10}).$$

By Gauss' genus theory the index of the subgroup

$$CL^2(-40n) := \{\alpha^2 \mid \alpha \in CL(-40n)\}$$

in $CL(-40n)$ is $2^{t(n)+1}$. Therefore for the known odd integers not of the form $x^2+y^2+10z^2$, (6) and the Birch and Swinnerton-Dyer Conjecture imply the following tantalizing equality relating class groups and Tate-Shafarevich groups:

$$|CL^2(-40n) \times CL^2(-40n)| = |Ш(E(-10n))|. \tag{7}$$

From our discussion, Ramanujan's search for a "simple law" leads to several deep theorems and conjectures in arithmetic geometry. To reiterate, if n equals 679, 2719, or one of the integers on Ramanujan's list, then using Shimura's lift, the Shimura-Taniyama correspondence, and the works of Kolyvagin and Waldspurger, we have obtained the following gems:

(i) There are no rational numbers x and y with $y \neq 0$ for which

$$y^2 = x^3 - 10nx^2 + 400n^2x - 4000n^3.$$

(ii) Assuming the Birch and Swinnerton-Dyer Conjecture,

$$|CL^2(-40n) \times CL^2(-40n)| = |Ш(E(-10n))|.$$

There are a few other ternary forms that also have such elegant properties, but most do not. This illustrates again how Ramanujan's deep insight continues to thrive beyond his centenary. By the way, Ramanujan's lifespan was 188**7**-**192**0.

Acknowledgements

The author thanks B. C. Berndt and J. H. Silverman for their helpful comments during the preparation of this article, and he also thanks the Institute for Advanced Study for their hospitality during the 1995-1996 and 1996-1997 academic years. The author's research is supported in part by NSF grants DMS-9304580 and DMS-9508976.

References

1. J. Benham and J. Hsia, Spinor equivalence of quadratic forms, *J. Number Th.* **17** (1983), 337-342.
2. W. Duke, Some old problems and new results about quadratic forms, *Notices Amer. Math. Soc.* **44** (1997), 190-196.
3. W. Duke and R. Schulze-Pillot, Representations of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids , *Invent. Math.* **99** (1990), 49-57.
4. V.A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and the Tate-Shafarevich group of $E(\mathbb{Q})$ for a subclass of Weil curves (Russian), *Izv. Akad. Nauk, USSR, ser. Matem.* **52** (1988), 522-540.
5. K. Ono and K. Soundararajan, Ramanujan's ternary quadratic form, *Invent. Math., to appear.*
6. S. Ramanujan, On the expression of a number in the form $ax^2 + by^2 + cz^2 + du^2$, *Proc. Cambridge Phil. Soc.* **19** (1916), 11-21.

7. G. Shimura, On modular forms of half-integral weight , *Ann. Math.* **97** (1973), 440-481.
8. J. H. Silverman, Taxicabs and sums of two cubes, *Amer. Math. Monthly* **100** (1993), 331-340.
9. J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer Verlag, New York, New York, 1992.
10. J.-L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures et Appl.* **60** (1981), 375-484.

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu