Counting solutions to equations in number theory

On 19 June I attended the 2014 Rouse Ball lecture by Richard Taylor, a British mathematician who played a big part in the proof of Fermat's Last theorem eventually completed by Andrew Wiles. Taylor is now at Princeton university in the USA.

He was discussing problems in "clock arithmetic" (called, in the textbooks, "modular arithmetic".

Take an ordinary clock face, only with 0 instead of 12. When you add hours on that clock:

$$11 + 3 = 2 \mod 12$$

You can also multiply in that arithmetic

e.g. $$11 \times 3 = 9 \mod 12$$

Most important is modular arithmetic with a prime number p of "hours" on the "clock face". In arithmetic modulo p, all the usual laws of arithmetic apply and you can do division sums (except dividing by 0)

Eg $$1 \div 3 = 2 \mod 5$$
$$2 \div 3 = 4 \mod 5$$
$$3 \div 3 = 1 \mod 5$$
$$4 \div 3 = 3 \mod 5$$

Marcus du Sautoy mentioned these clock-arithmetic mathematical structures when he came to speak on group theory.

What about quadratic equations in clock arithmetic?

Eg. When does $x^2 = n \mod p$ have a solution?

Answer: first see that it will be enough to find when $x^2 = q \bmod p$ has a solution for q prime.

A number n for which $x^2 = n \bmod p$ has a solution is (for odd reasons) called a residue.

- If a and b are residues, ab is
  (if $a = A^2 \bmod p$, and $b = B^2 \bmod p$
  $ab = A^2B^2 \bmod p$).
- If a is a residue and b isn't, then ab isn't.
  (if $ab = d^2 \bmod p$ and $a = c^2 \bmod p$
  then $b = (d/c)^2$, so b is a residue)
- For all $a < p$, $(p-a)^2 = a^2 \bmod p$ ∴ each residue is the square of 2 distinct numbers mod p ∴ half the numbers $1, 2, 3 \ldots (p-1)$ are residues (for any odd prime p)
- If a and b are both not residues, then ab is a residue.
  (ab goes through $(p-1)$ different values, ie. all the numbers $1, 2, 3 \ldots (p-1)$ in some order, as b goes through $1, 2, 3 \ldots (p-1)$. Half those values of ab are non-residues, i.e. those when b is a residue ∴ those when b is a non-residue must be residues).

Hence if n is composite, it is a non-residue if and only if an odd number of primes in its prime factorisation are non-residues

Eg mod 17, 15 is a residue because 3 isn't and 5 isn't
12 isn't a residue because 3 isn't, 2 is, 2 is.

So we want to find when

$x^2 = q \bmod p$ has a solution for q and p prime and odd

Answer (Gauss's quadratic reciprocity theorem)

If either of p or q is of form $4n+1$, then

q is a residue mod $p \iff p$ is a residue mod q

If both p and q are of form $4n+3$, then

q is a residue mod $p \iff p$ is <u>not</u> a residue mod q

Example Does $x^2 = 3 \bmod 20142013$ have a solution?

We could find out by checking all 20 million odd numbers $1, 2, 3 \ldots 20142012$, squaring each one and seeing if the answer is $= 3 \bmod 20142013$, but it would be laborious (about six years' work if you work on it solidly 8 hours a day, 365 days a year, checking a number every 3 seconds).

Quicker: $x^2 = 3 \bmod 20142013$ has a solution if and only if $x^2 = 20142013 \bmod 3$

$= 1 \bmod 3$ has a solution

Since 20142013 has remainder 1 when divided by 4

Now $x^2 = 1 \bmod 3$ obviously has a solution

$\therefore$ $x^2 = 3 \bmod 20142013$ has a solution

(though we don't know what it is)

(20142013 is a prime number:

www.isprimenumber.com/prime/20142013.

$x^2 = 3 \bmod 20142019$ does <u>not</u> have a solution.)

Richard Taylor said that even after studying many different proofs of the quadratic reciprocity theorem, he still can't see why it *should* be true, as distinct from knowing that it just *is* true (because it has been proved)

After all, one of the basic things about primes is that knowing the first 100, or 1000, primes does not tell you at all what the 101st or 1001st is. Each prime is "on its own". So why should residues mod 2014 2013 have any connection with residues mod 3?

Richard Taylor said he found the proof via Gauss sums:
www.math.uiuc.edu/~r-ash/Ant/AntApp.pdf
the most illuminating (when I asked him after the lecture) — but the question is still obscure to him. Anyone who can work out a *new* proof of the theorem which illuminates more will be advancing maths a lot.

* * *

Besides "reciprocity theorems", like Gauss's, which help us identify values of q for which

$$x^2 = q \mod p$$

has a solution, there are "density theorems".

The Dirichlet density theorem, further developed by de la Vallée Poussin, says:

If n is not a perfect square, then

$$X^2 = n \mod p$$

has two solutions for half the prime numbers, and zero solutions for half. (This is sort of what you'd expect if prime numbers are half $4n+1$ types, and half $4n+3$ types).

Eg. $x^2 = 3 \bmod p$
has a solution for $\alpha(N)$ of the primes $\leq N$
and $\alpha(N) \to \frac{1}{2}$ as $N \to \infty$

Corollary: n is a perfect square if and only if
n is a perfect square mod <u>all</u> p.

Eg. 4 is a perfect square, and a square mod 5, 7, 11, 13, 17...
and so on for ever.

5 is a square mod 11, because $4^2 = 5 \bmod 11$,
and 5 is a square mod 19, 29, 31, 41... (i.e. it's a square
mod p for five of the first 12 odd primes $p > 5$), and
as we go on the proportion of primes for which 5 is a
square gets close to $1/2$; but there is no number which
turns out to be a square mod p for all p which is
not itself a perfect square (1 or 4 or 9 or 16 or...)

* * *

As part of the famous Langlands programme — a series of
conjectures about connections between number theory and
algebra (meaning, by "algebra", group theory and
developments from it, not what we call "algebra" in school),
made by Robert Langlands in the 1960s
— en.wikipedia.org/wiki/Robert_Langlands —
conjectures have been made about reciprocity theorems for
cubic, quartics, quintics, equations of degree 6, etc.

But very few of those conjectures have been proved.

* * *

Some results have been proved about numbers of solutions (mod p) to some equations in two variables, notably elliptic curves

$$Y^2 = X^3 + cX + d \qquad [1]$$

(These "elliptic curves" are not ellipses, and in fact have a fairly distant connection to ellipses. But they've been important in number theory since the 1870s).

Then let N_p = number of solutions mod p

Hasse proved: $|p - N_p| < 2\sqrt{p}$

For the equation $Y^2 + Y = X^3 - X^2$ [2]
(which is actually only a rejigged version of an equation like [1]) Eichler proved:

$p - N_p$ = coefficient of q^p in expansion of

$$\prod_1^\infty (1-q^n)^2 (1-q^{11n})^2$$

* * *

Taylor then talked about the Taniyama conjecture, famous in its own right and also as the crucial step in Taylor's and Wiles's work to prove Fermat's last theorem.

The conjecture (now, since it's been proved, called the modularity theorem) says that any elliptic curve which includes a point with all-rational coefficients is equivalent to a modular form (which is a differentiable function with some symmetry properties defined in terms of a group of 2×2 matrices).

then if $$f(\tau) = \prod_1^\infty (1-q^n)^2(1-q^{11n})^2$$

and $q = e^{2\pi i \tau}$

then the product converges for $\mathrm{Im}(\tau) > 0$ and if $f(\tau)$ is written out as:

$$f(\tau) = \sum_1^\infty a_n e^{2\pi i n \tau} \quad \text{(Fourier series)}$$

then $a_p = p - N_p$ for all p.

Not much is known about the significance of a_n for n not prime.

* * *

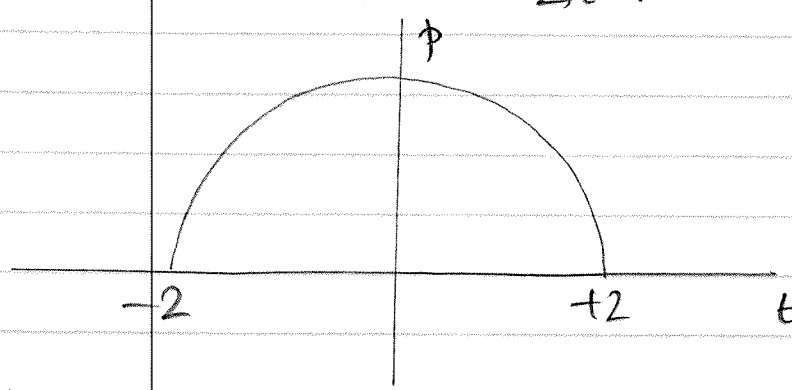
If t is defined as the error term

$$t = (p - N_p)/\sqrt{p}$$

Then we know from Hasse's theorem that $-2 \le t \le 2$

And we can show that as $p \to \infty$ the distribution of t approaches

$$\mathrm{pdf}(t) = \frac{1}{2\pi}\sqrt{4-t^2}$$



Taylor 18

the proof of the Taniyama conjecture, as Taylor told us, depends on "infinite Galois theory".

Basic Galois theory defines the Galois group of a polynomial P

G = group of automorphisms (maps of itself into itself which preserve all the relations in arithmetic, sums, products, and so on) of the field extension F, defined as the smallest field (mathematical structure inside which you can do normal addition, multiplication, etc.) which extends $\mathbb{Q}$ enough to include the roots of P.

then Galois's theorem of the impossibility of an algebraic formula to solve polynomial equations of degree ≥ 5 follows by looking at the Galois groups of those polynomials.

http://nrich.maths.org/1422

(this is what Marcus du Sautoy started his talk from).

the "infinite Galois theory" in the proof of the Taniyama conjecture involves constructing an "inverse limit" of all the Galois groups of polynomials with rational coefficients.