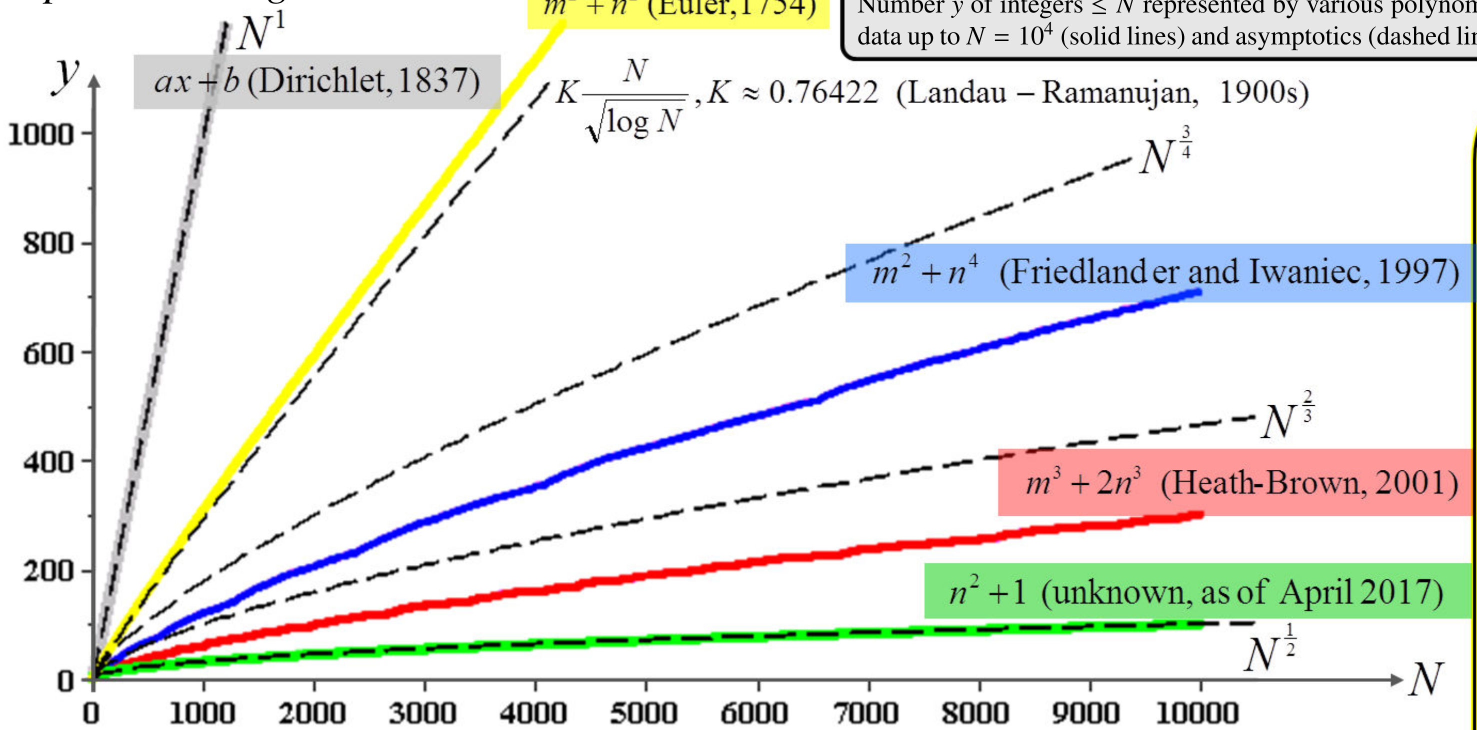
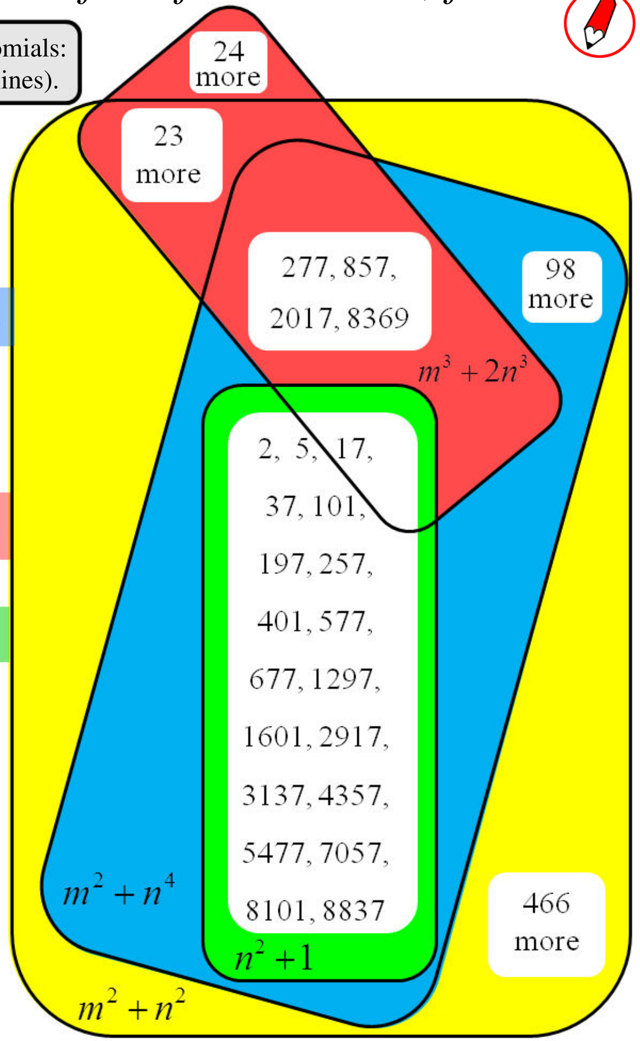
THEOREM OF THE DAY

The Friedlander–Iwaniec Theorem *There are infinitely many prime numbers of the form $m^2 + n^4$, for positive integers m and n.*



Number y of integers $\leq N$ represented by various polynomials: data up to $N = 10^4$ (solid lines) and asymptotics (dashed lines).



Venn diagram of primes less than 10^4 as represented by four polynomials. Only 17 is represented by all four.

Number theorists are morally certain that any reasonable polynomial $f(x_1, \ldots, x_t)$, in several positive integer variables and with integer coefficients, will take infinitely many prime values. Of course f must not factorise, and there are obvious so-called 'local conditions', e.g. $f(x) = x(x+1) + 2$ is excluded because one of x and $x + 1$ is even, forcing $f(x)$ to be even. To start with the one-variable linear prototype: $f(x) = ax + b$ produces infinitely many primes if and only if a and b are coprime. Legendre asserted this in 1785; its proof sixty years later by Dirichlet marks the birth of analytic number theory. Taking $a = 4$ and $b = 1$, we see that infinitely many primes have the form $4k + 1$ and these, as asserted by Girard and Fermat in the 16th century, are precisely the prime values of $f(x_1, x_2) = x_1^2 + x_2^2$. Although not easy to prove, Dirichlet's result is easy to achieve in the sense that the sequence $ax + b$, $x = 1, \ldots, N$, accounts for a proportion of about $1/a$ of the set $\{1, \ldots, N\}$. Up to a constant multiple this means that N^1 values from $\{1, \ldots, N\}$ are produced: we have marked this with the dashed line $y = N$ on the chart above left. The polynomial $x_1^2 + x_2^2$ is less generous, but the proportion, determined by Landau and Ramanujan, is nearly linear: this is marked as the dashed line $y = KN/\sqrt{\ln N}$, closely shadowing the actual count of integers $\leq N$ representable as $m^2 + n^2$, displayed on our chart up to $N = 10^4$. Contrast this with the other three polynomials: the sequences of integer values they produce constitute only a fraction of N^α of $\{1, \ldots, N\}$, with $\alpha < 1$ in each case. Such sequences are known as 'thin'.

Friedlander and Iwaniec used sophisticated prime 'sieving' methods to give the first proof that a thin polynomial sequence could contain infinitely many primes, inspiring Heath-Brown's proof that there are infinitely many primes which are sums of three cubes.

Web link: Iwaniec and Friedlander: www.pnas.org/content/94/4/1054.abstract; Heath-Brown: eprints.maths.ox.ac.uk/168.
Further reading: *Prime-Detecting Sieves* by Glyn Harman, Princeton University Press, 2007.
Read Chapter 1 at press.princeton.edu/titles/8585.html.