

Inria

Finding large smooth twins

Bruno Sterner

Inria Saclay and LIX, France

Talk for the lightning session at ANTS XVI

Consecutive integers

$$\begin{array}{rcl} \vdots & & \vdots \\ 22529735146513345759959448571 & = & 2137 \cdot 10542693096169090201197683 \\ 22529735146513345759959448572 & = & 2^2 \cdot 3 \cdot 907 \cdot 39239 \cdot 70177 \cdot 751717782012361 \\ 22529735146513345759959448573 & = & 97 \cdot 66533 \cdot 2653633 \cdot 1315547053747481 \\ 22529735146513345759959448574 & = & 2 \cdot 8423 \cdot 296591 \cdot 4132577 \cdot 1091139724967 \\ 22529735146513345759959448575 & = & 3^2 \cdot 5^2 \cdot 7^5 \cdot 11^3 \cdot 59 \cdot 71^2 \cdot 101 \cdot 127 \cdot 173^2 \cdot 197 \cdot 199 \\ 22529735146513345759959448576 & = & 2^{10} \cdot 13 \cdot 17^2 \cdot 23 \cdot 37^2 \cdot 41 \cdot 47 \cdot 61 \cdot 79 \cdot 107^2 \cdot 113^2 \cdot 137 \\ 22529735146513345759959448577 & = & 4515076051 \cdot 4989890511705435227 \\ 22529735146513345759959448578 & = & 2 \cdot 3 \cdot 29 \cdot 10273 \cdot 12604033531997919868039 \\ 22529735146513345759959448579 & = & 73 \cdot 308626508856347202191225323 \\ 22529735146513345759959448580 & = & 2^2 \cdot 5 \cdot 499 \cdot 599623 \cdot 3764846397877672777 \\ \vdots & & \vdots \end{array}$$

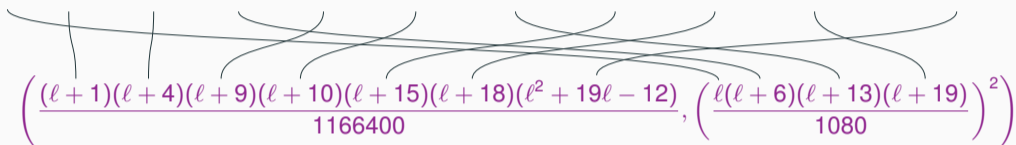
“smooth twin”

Can we find large (≥ 240 -bit) smooth twins? Such twins should exist with smoothness bounds $B > 1200$ but it is computationally infeasible to find them

Overview of our approach

For $\ell = 38295031104$, all of these are 43000-smooth:

ℓ $\ell+1$ $\ell+4$ $\ell+6$ $\ell+9$ $\ell+10$ $\ell+13$ $\ell+15$ $\ell+18$ $\ell+19$ $\ell^2+19\ell-12$



A diagram consisting of a horizontal line with several vertical tick marks. Curved lines connect these tick marks to the terms in the equation below: ℓ to 1166400 , $\ell+1$ to $(\ell+1)$, $\ell+4$ to $(\ell+4)$, $\ell+6$ to $(\ell+6)$, $\ell+9$ to $(\ell+9)$, $\ell+10$ to $(\ell+10)$, $\ell+13$ to $(\ell+13)$, $\ell+15$ to $(\ell+15)$, $\ell+18$ to $(\ell+18)$, $\ell+19$ to $(\ell+19)$, and $\ell^2+19\ell-12$ to $(\ell^2+19\ell-12)$.

$$\left(\frac{(\ell+1)(\ell+4)(\ell+9)(\ell+10)(\ell+15)(\ell+18)(\ell^2+19\ell-12)}{1166400}, \left(\frac{\ell(\ell+6)(\ell+13)(\ell+19)}{1080} \right)^2 \right)$$

This is a 262-bit smooth twin since the following polynomials differ by $C = 1166400$

$f(x) = (x+1)(x+4)(x+9)(x+10)(x+15)(x+18)(x^2+19x-12)$, and

$g(x) = x^2(x+6)^2(x+13)^2(x+19)^2$

Thanks for listening and enjoy ANTS!

