Faster number theory with smaller numbers

Marco Streng

This week's discoveries
16-04-2013

- Mathematisch Instituut, Universiteit Leiden (started 1st April 2013)
- NWO Veni
- before:
  - VU Amsterdam
  - Warwick (UK)
  - Microsoft Research (USA)
  - Leiden

A number theory problem

Question

Which prime numbers p can be written as a sum of two squares?

$$(p = x^2 + y^2 \qquad \text{with integers } x \text{ and } y)$$

Examples

- $5 = 2^2 + 1^2$
- $3 \neq x^2 + y^2$

A number theory problem

Question

Which prime numbers p can be written as a sum of two squares?

$$(p = x^2 + y^2 \qquad \text{with integers } x \text{ and } y)$$

Examples

- $5 = 2^2 + 1^2$
- $3 \neq x^2 + y^2$

Answer

The primes p such that the equation

$$u^2 + 1 = 0$$

has a solution modulo p.

"Local answer": only in terms of remainders after division by p.

A variant

Question

Which prime numbers p can be written as

$$p = x^2 + 71y^2 \qquad \text{with integers } x \text{ and } y?$$

Examples

- $293 = 3^2 + 71 \cdot 2^2$
- $311 \neq x^2 + 71 \cdot y^2$

Answer

The primes p such that the equations

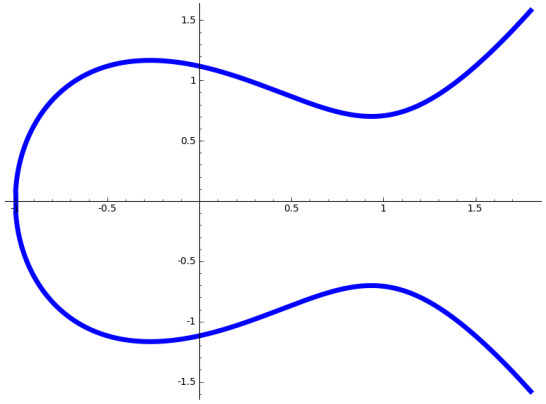
$$u^2 + 71 = 0 \qquad \text{and} \qquad f(v) = 0$$

have solutions modulo p.
Here $f(v)$ is some fixed polynomial of the form

$$f(v) = v^7 + a_6 v^6 + a_5 v^5 + a_4 v^4 + a_3 v^3 + a_2 v^2 + a_1 v + a_0.$$

Where does f come from?

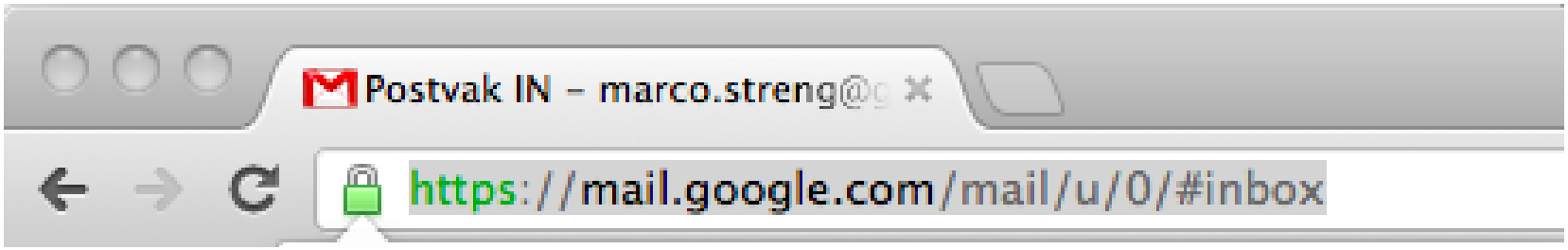
Theory of elliptic curves with complex multiplication.



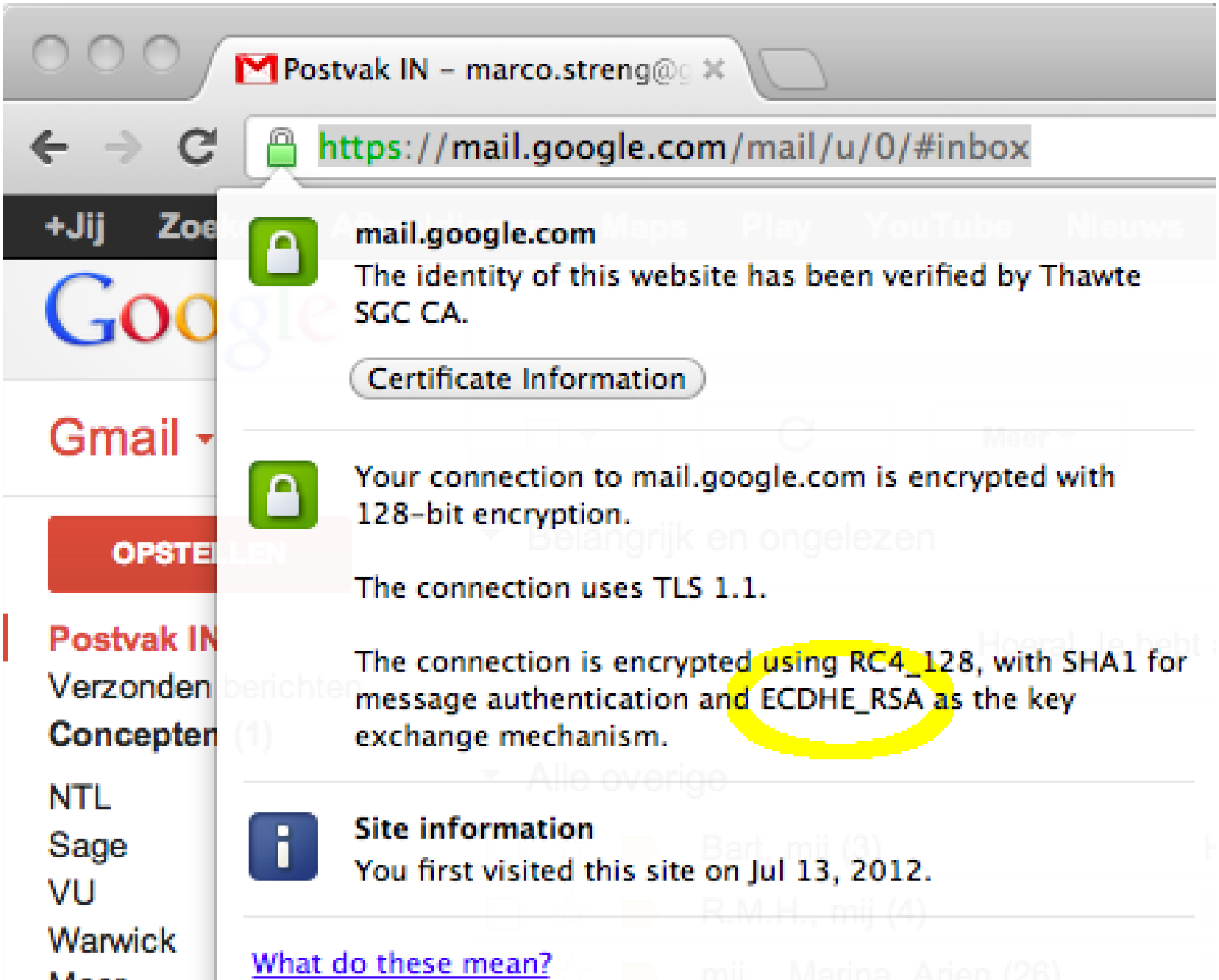
$$Y^2 = X^3 + aX + b$$

Applications:

- Number theory (as previous slides)
- Create efficient and secure cryptography systems using f: elliptic curve cryptography



Google uses elliptic curves



The theory gives us a polynomial $f(v)$:

$$
\begin{aligned}
& v^7 - 983737006030905231997 15v^6 \\
& - 45469516979819231769564486769 86v^5 \\
& - 20990393987344602049551931659611827275 8v^4 \\
& - 12543980353722772760179537174109237891242365v^3 \\
& - 28231047451814704248363459970244920935716010360 6v^2 \\
& + 90433020636775262252632416040884979791008930009 4965v \\
& - 70982259781561678856146099997145588988479357689323263
\end{aligned}
$$

For each integer n, have an equation $p = x^2 + ny^2$, and a polynomial f.
Complexity of f is exponential in the complexity of n.

Weber ($\sim$ 1900) can also use:

$$v^7 + v^6 - v^5 - v^4 - v^3 + v^2 + 2v - 1$$

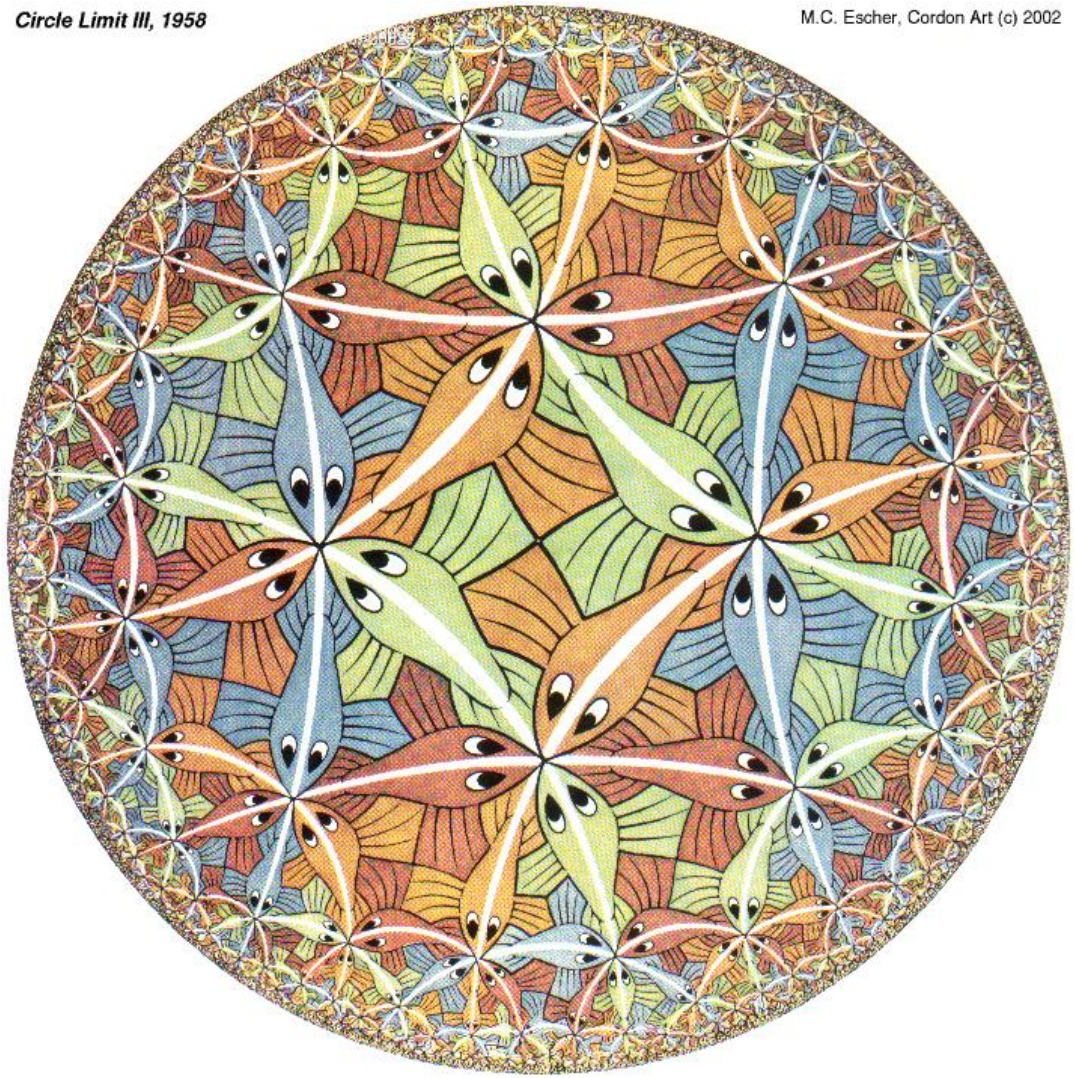
Methods: modular forms and symmetries

Let $\eta(z) = q^{1/24} \prod_{n=1}^{\infty}(1-q^n)$, where $q = e^{2\pi i z}$.

$$\eta(z+1) = e^{\pi i/12}\ \eta(z),$$
$$\eta(-1/z) = \sqrt{-iz}\ \eta(z)$$

Let $g(z) = e^{-\pi i/24}\sqrt{2}\,\dfrac{\eta(z)}{\eta(\frac{z-1}{2})}$.

- Number $\alpha = g(i\sqrt{71})$.
- Turns out to be algebraic, i.e., $f(\alpha) = 0$ for some "nice" polynomial $f(v)$.
- This is Weber's $f(v)$!



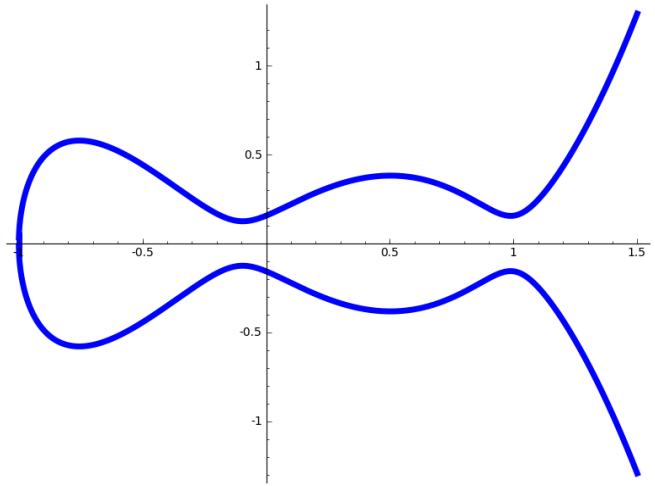
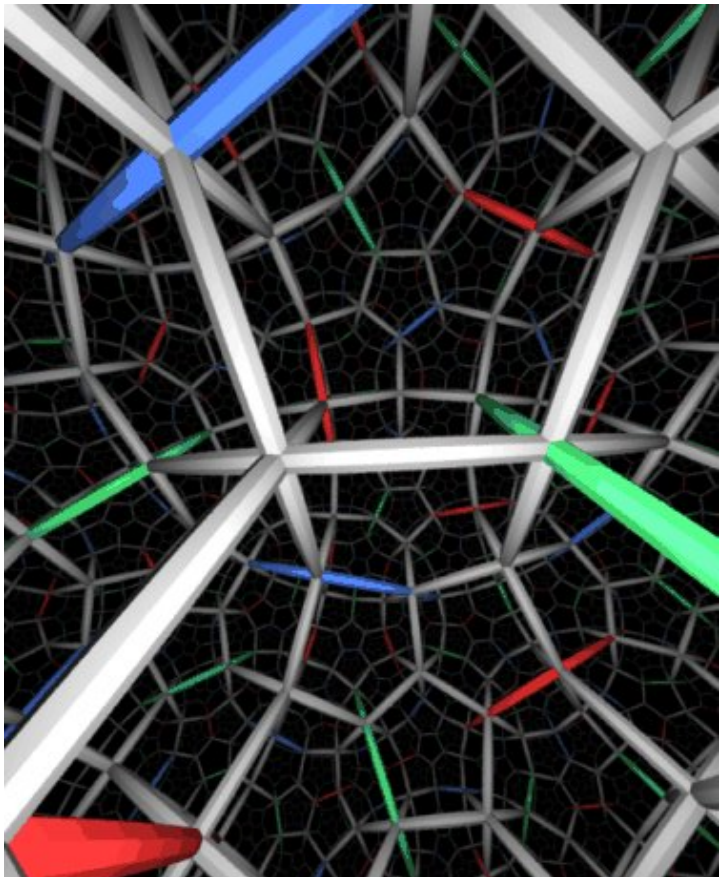
key: Shimura's reciprocity law relates symmetries of this picture to symmetries of roots of polynomials

Higher-dimensional analogue

By considering general curves, we get

- access to more number theory problems,
- an alternative to elliptic curve cryptography.

Question: Can we make the polynomials smaller there too?

Tools: modular forms for higher-dimensional analogues of the Escher picture.

- I gave an explicit higher-dimensional reciprocity law and preliminary examples.
- This is the start of next week's discoveries.