Numbers and Entropy

John Mangual

Fermat[1] showed that any $p = a^2 + b^2$ has a solution for p prime and integers a, b iff $p = 4k + 1$. Primes can be arbitrarily large, how do we find (a, b)?

Algorithm #1

- Let x be quadratic non-residue and set $z = x^{\frac{p-1}{4}} + i$
- Then $a + ib = \gcd(x^{\frac{p-1}{4}} + i, p)$

Algorithm #2

- Let $(\frac{a}{p})$ be the Legendre symbol[2].
- $a = \sum_{0 \leq x < p} (\frac{x^3 - x}{p})$

Algorithm #3 Let $c = \sqrt{-1} \mod p$ and $\gcd(p, i - c) = a + bi$ then $p = a^2 + b^2$.

- Somehow need to compute $\sqrt{-1}$ (maybe theory of Pell's eq)
- need GCD algorithm in $\mathbb{Z}[i]$.

Algorithm #4

- Find $z^2 = -1 \mod p$.
- Take Euclidean algorithm of (z, p) until $x, y < \sqrt{p}$

Algorithm #5

- Find $x = \frac{1}{2}\binom{2k}{k} \mod p$ and let $y = x \cdot (2k)! \mod p$
- Why are $x, y < \frac{p}{2}$? Gauss showed $x^2 + y^2 = p$ (that is not a congruence).

1 Prime Number Theorem

What happens to these algorithms as $p \to \infty$? No freaking idea.

[1] **Efficiently finding two squares which sum to a prime** http://math.stackexchange.com/q/5877/4997
[2] **Explicit formula for Fermat's $4k + 1$ theorem** http://math.stackexchange.com/a/74299/4997

References

[1] Jean Bourgain, Alex Kontorovich.
Beyond Expansion II: Low-Lying Fundamental Geodesics arXiv:1406.1366
Beyond Expansion II: Traces of Thin Semigroups arXiv:1310.7190

[2] Dubi Kelmer. *Quadratic irrationals and linking numbers of modular knots* arXiv:1205.2230

[3] Menny Aka, Uri Shapira. *On the evolution of continued fractions in a fixed quadratic field* arXiv:1201.1280

[4] Curtis McMullen *Uniformly Diophantine numbers in a fixed real quadratic field* http://www.math.harvard.edu/~ctm/papers/home/text/papers/cf/cf.pdf