Finding the four squares in Lagrange's Theorem

Enrique Treviño

joint work with Paul Pollack

Joint Math Meetings
January 11, 2018

LAKE FOREST
COLLEGE

Coauthors

(a) Paul Pollack

Theorem (Lagrange, 1770)

Every positive integer n can be written as a sum of four squares.

Questions:

- For a given n, how do we find these squares?
- How fast can we do it?

Main Result

Rabin and Shallit in 1986 presented three random algorithms with the following expected runtimes:

1. $O((\log n)^2)$ (this one depends on ERH and was discovered by Rabin in 1977)
2. $O((\log n)^2 \log\log n)$
3. $O((\log n)^2(\log\log n)^2)$

Theorem (Pollack-T)

There are two random algorithms with expected runtime

$$O\left(\frac{(\log n)^2}{\log\log n}\right).$$

One algorithm is dependent on ERH and one is not.

Integral Quaternions

Let i, j, k satisfy $i^2 = j^2 = k^2 = -1$ and $ij = k, jk = i, ki = j$. The Hurwitz integral quaternions are:

$$\mathbb{H} := \{\frac{1}{2}(a + bi + cj + dk) : a, b, c, d \in \mathbb{Z}, a \equiv b \equiv c \equiv d \pmod 2\}.$$

Let $\alpha = a + bi + cj + dk$, then the **norm** of α is $N\alpha = a^2 + b^2 + c^2 + d^2$.

Lemma

n is a sum of four squares if and only if $n = N\alpha$ for some $\alpha \in \mathbb{H}$.

Reduction to norms

$$\mathbb{H} := \{\frac{1}{2}(a + bi + cj + dk) : a, b, c, d \in \mathbb{Z}, a \equiv b \equiv c \equiv d \pmod 2\}.$$

Lemma

n is a sum of four squares if and only if $n = N\alpha$ for some $\alpha \in \mathbb{H}$.

Proof.

- Suppose $a \equiv b \equiv c \equiv d \equiv 1 \bmod 2$.
- Choose $\epsilon_a, \epsilon_b, \epsilon_c, \epsilon_d \in \{\pm 1\}$ so that

$$\epsilon_a \equiv a, \quad \epsilon_b \equiv -b, \quad \epsilon_c \equiv -c, \quad \epsilon_d \equiv -d \pmod 4.$$

- Let $\epsilon = \frac{1}{2}(\epsilon_a + \epsilon_b i + \epsilon_c j + \epsilon_d k)$
- Then $\beta = \alpha\epsilon = A + Bi + Cj + Dk$ with $A, B, C, D \in \mathbb{Z}$ and $N\beta = N\alpha$.

$\square$

Useful Lemma

Lemma

Let n be an odd positive integer. If $n \mid N(a + bi + cj + dk)$, where $\gcd(a, b, c, d) = 1$, then any gcrd of n and $a + bi + cj + dk$ has norm n.

Note: Quaternions are not commutative, so you can have right greatest common divisors and left greatest common divisors.

Rabin Algorithm depending on ERH

1. Reduce to the odd part:
   - Write $n = 2^e n'$. Takes at most $O(\log n)$ steps.
   - Suppose $X'^2 + Y'^2 + Z'^2 + W'^2 = n'$, then

$$(1+i)^e(X' + Y'i + Z'j + W'k) = X + Yi + Zj + Wk.$$

2. Assume n is odd. **Find** prime $p < (2n)^5$ such that $p \equiv -1 \pmod{n}$ and $p \equiv 1 \pmod{4}$.
   - Find A, B such that $p = A^2 + B^2$.
   - Then $n | p + 1 = A^2 + B^2 + 1 = N(A + Bi + j)$.
3. Compute $\mathrm{gcrd}(n, A + Bi + j)$.

Why ERH is needed?

"**Find** prime $p < (2n)^5$ such that $p \equiv -1 \pmod{n}$ and $p \equiv 1 \pmod{4}$."

Under ERH, among all integers up to $(2n)^5$ that are $\equiv -1 \pmod{n}$ and $\equiv 1 \pmod{4}$, the proportion of primes is $\gg \frac{n}{\varphi(n)} \cdot \frac{1}{\log n} \gg \frac{1}{\log n}$. So we expect to hit a prime p in $O(\log n)$ trials.

Big Idea

The proportion of primes p such that $p \equiv -1 \pmod{n}$, $p \equiv 1 \pmod{4}$ smaller than $(2n)^5$ is $\gg \frac{n}{\varphi(n)} \cdot \frac{1}{\log n} \gg \frac{1}{\log n}$

Exploit the variability in the ratios $\frac{n}{\varphi(n)}$.

Final Algorithm

(1) [Precomputation] Determine the primes not exceeding $\log n$ and compute their product M.

(2) [Random trials] Choose an odd number $k < n^5$ at random, and let

$$p = Mnk - 1.$$

(Notice that $p \equiv 1 \pmod 4$, since $2 \parallel M$ and n, k are odd.) For a randomly chosen $u \in [1, p-1]$, compute $s = u^{(p-1)/4} \operatorname{Mod} p$ and test if $s^2 \equiv -1 \pmod p$. If so, continue to the next step. Otherwise, restart this step.

(3) [Denouement] Compute $A + Bi := \gcd(s + i, p)$. Then compute $\mathrm{gcrd}(A + Bi + j, n)$, normalized to have integer components. Write this gcrd as $X + Yi + Zj + Wk$, and output that $n = X^2 + Y^2 + Z^2 + W^2$.

How does the non-ERH one work?

(0) Calculating sum of two scares for “small primes”.

- Flag each number in $[1, \log n]$ as prime or composite using $O((\log n)^{3/2})$ operations.
- Compute $X^2 + Y^2$ for all pairs X, Y with $0 \leq X, Y \leq (\log n)^{1/2}$.
- Record, for $\ell = 2$ and for the primes $\ell \leq \log n$ with $\ell \equiv 1 \pmod 4$, integers X_ℓ, Y_ℓ with

$$\ell = X_\ell^2 + Y_\ell^2.$$

Continuation

(1) Select x, y at random from $[1, N]$ and compute

$$r := (-(x^2 + y^2)) \operatorname{Mod} N.$$

- There are $\gg N(\log\log n)^{1/2}/\log N$ integers in $[1, N]$ that have the form $r_1 p$, where r_1 is a product of primes $\ell \leq \log n$ with $\ell \equiv 1 \pmod 4$, and $p > \log n$ is a prime congruent to 1 modulo 4 not dividing N.
- The number of choices for x, y where r lands on one of the numbers $r_1 p$ is

$$\gg N^2 \frac{\log\log n}{\log N} \gg N^2 \frac{\log\log n}{\log n}.$$

- Thus, we expect to have $r = r_1 p$ within $O(\log n/\log\log n)$ trials.

(2) Having located $r = r_1 p$, compute a two-squares representation of r_1:

$$u^2 + v^2 = r_1, \quad \text{where} \quad u + vi := \prod_{\ell^{v_\ell} \| r_1} (X_\ell + Y_\ell i)^{v_\ell}.$$

(3) Suppose we have written $p = U^2 + V^2$, and let $z + wi = (u + vi)(U + Vi)$. Then

$$-(x^2 + y^2) \equiv r = r_1 p = z^2 + w^2 \pmod{N},$$

so that

$$n \mid N \mid x^2 + y^2 + z^2 + w^2.$$

(4) Compute $\mathrm{gcrd}(n, x + yi + zj + wk)$. BAM!

Thank you!