Irregular primes to two billion: progress report

David Harvey

University of New South Wales

5th October 2013, CARMA, University of Newcastle

Contents

- A big computation
- Theoretical background
- Algorithms

A big computation

Primary goal: compute all irregular primes up to $2^{31} = 2{,}147{,}483{,}648$.

Total computation time so far:

$$\begin{aligned} 7 \text{ million core-hours} &\approx 800 \text{ core-years} \\ &\approx 1000 \text{ cores running for 9 months} \end{aligned}$$

Should be finished in a few weeks.

Some other large number-theoretic efforts:

- RSA-768, 2009: about 2000 years
- Zetagrid, 2003: about 2300 years
- Certicom ECC Challenge, 2002: about 15000 years
- PrimeGrid: about 3 million years (?) on various projects

Does anyone know any others? Maybe someone should be keeping track?

Machines used:

location	cluster	cores	hours × 1000
UNSW	Condor	636	1,840
	Katana	1280	1,373
	Tensor	336	662
NYU	Union Square	584	217
	Bowery	2528	714
	Cardiac	1264	406
NCI (ANU)	Vayu	11936	94
	Raijin	57472	281
Intersect	Orange	1600	1,370

RAM per node varies widely, from 16GB to 256GB.

Also performance varies widely between clusters!!

Theoretical background

Recall the Bernoulli numbers

$$\frac{x}{e^x - 1} = \sum_{k \geq 0} \frac{B_k}{k!} x^k.$$

Here are the first few:

$$\begin{aligned} B_0 &= 1 & B_1 &= -1/2 \\ B_2 &= 1/6 & B_3 &= 0 \\ B_4 &= -1/30 & B_5 &= 0 \\ B_6 &= 1/42 & B_7 &= 0 \\ B_8 &= -1/30 & B_9 &= 0 \\ B_{10} &= 5/66 & B_{11} &= 0 \\ B_{12} &= -691/2730 & B_{13} &= 0 \\ B_{14} &= 7/6 & B_{15} &= 0 \end{aligned}$$

Definition due to Kummer:

An odd prime p is **irregular** if it divides one of

$$B_2, B_4, \ldots, B_{p-3}.$$

Otherwise it is **regular**.

Kummer could prove many cases of Fermat's Last Theorem for regular primes.

The first irregular prime is $p = 37$:

$$37 \mid B_{32} = \frac{-7709321041217}{510}.$$

We call $k = 32$ an **irregular index** for $p = 37$.

There is a close connection with the cyclotomic field $K = \mathbf{Q}(\zeta_p)$.

Let A be the p-part of the class group of K.

Then $G = \mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ acts on A, where $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ corresponds to $\sigma_a : \zeta \mapsto \zeta^a$.

Let $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times$ be the Teichmüller character.

Regard A as a $\mathbf{Z}_p[G]$-module. It splits into eigenspaces

$$A = \bigoplus_{i=0}^{p-2} e_i A$$

where the orthogonal idempotents are

$$e_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a) \sigma_a^{-1} \in \mathbf{Z}_p[G], \qquad 0 \le i \le p-2.$$

In other words $e_i A$ is the submodule where σ_a acts as $\omega^i(a)$ for all a.

Ribet's theorem:

$$p \mid B_k \iff e_{p-k}A \neq 0, \qquad k = 2, 4, \ldots, p-3.$$

So irregular indices correspond precisely to nontrivial (odd) eigenspaces.

Example for $p = 37$ and $k = 32$:

Take $\mathfrak{p} = (149, \zeta - 6)$, a degree 1 prime ideal lying over $q = 149$.

(Note $149 = 1 \pmod{37}$ and $6^{37} = 1 \pmod{149}$).

Bit harder to see: K has class number 37, and $\mathfrak{p}$ is non-principal.

Ribet's theorem says that the class of $\mathfrak{p}$ lies in $e_5 A$.

In other words, for any $a \in (\mathbf{Z}/37\mathbf{Z})^\times$, the ideal quotient

$$\mathfrak{p}^{\omega^5(a)-\sigma_a} = \mathfrak{p}^{a^5}/(149, \zeta^a - 6)$$

is principal. Your favourite computer algebra system agrees!

The **even** eigenspaces are much more mysterious.

The Kummer–Vandiver conjecture asserts that

$$e_{p-k}A = 0, \qquad k = 3, 5, \ldots, p-2.$$

Known to be true for $p < 163{,}577{,}856$ (Buhler–H. 2011).

Current project will extend this to $p < 2^{31}$.

Some heuristics suggest $O(\log \log x)$ counterexamples for $p < x$.

Other heuristics suggest $O(1)$ counterexamples for $p < x$.

The theoretical problem is too hard for me...

So I just keep searching!

Algorithms

Goal: given p, compute $B_0, B_2, \ldots, B_{p-3} \pmod{p}$.

Naive algorithms (pre-1990s) have complexity $O(p^2)$.

The first $p^{1+o(1)}$ algorithm deployed for this problem was the **series inversion** algorithm.

Idea: write down the series

$$\frac{e^x - 1}{x} = 1 + \frac{1}{2!}x + \frac{1}{3!}x^2 + \cdots + \frac{1}{(p-2)!}x^{p-3} + O(x^{p-2}),$$

and invert it up to $O(x^{p-2})$, working over $\mathbf{F}_p$.

Can save a factor of two in time and space by using identities like

$$\frac{x^2}{\cosh x - 1} = -2 + \sum_{n=0}^{\infty} \frac{(2n-1)B_{2n}}{(2n)!}x^{2n}.$$

Further savings in memory (and a little time) are obtained via more elaborate identities.

Using Newton's method, series inversion reduces to polynomial multiplication.

So ultimately this method depends on fast multiplication of polynomials of degree $O(p)$ over $\mathbf{F}_p$.

A second method depends on a **Voronoi congruence**:

$$\begin{aligned}\frac{2(2^{2n}-1)}{2n}B_{2n} &= \sum_{j=1}^{p-1}(-1)^{j-1}j^{2n-1} \pmod p \\ &= 1^{2n-1} - 2^{2n-1} + \cdots - (p-1)^{2n-1} \pmod p.\end{aligned}$$

If $2^{2n} \neq 1 \pmod p$, this recovers $B_{2n} \pmod p$.

If $2^{2n} = 1 \pmod p$, we have a problem.

There are workarounds — let's ignore this today.

Let us rearrange into 'multiplicative' order.

Choose a generator $g \in (\mathbf{Z}/p\mathbf{Z})^\times$ and make the substitution $j = g^i$.

Write $a_i = (-1)^{(g^i \bmod p)-1}$. Note that $a_{i+(p-1)/2} = -a_i$.

Sum becomes

$$\sum_{i=0}^{(p-3)/2} a_i g^{-i} g^{2ni}.$$

We now recognise this as the **discrete Fourier transform** of the sequence

$$\{a_i g^{-i}\}_{i=0}^{(p-3)/2}$$

of length $(p-1)/2$ over $\mathbf{F}_p$ with respect to g^2.

Example: for $p = 37$ and $g = 2$, the a_i sequence is

$$(+1, -1, -1, -1, -1, -1, +1, +1, -1, +1, +1, +1, -1, +1, -1, +1, +1, -1)$$

The sequence $\{a_i g^{-i}\}$ is

$$(1, 18, 9, 23, 30, 15, 11, 24, 25, 6, 3, 20, 27, 5, 16, 29, 33, 2)$$

and its DFT with respect to $g^2 = 4$ is

$$(1, 28, 23, 28, 29, 17, 20, 24, 11, 13, 24, 17, 11, 18, 18, 13, 0, 19).$$

The zero corresponds to $n = 16$ and thus the irregular index $2n = 32$.

But how do we efficiently compute a DFT over $\mathbf{F}_p$?

We would like to use a Fast Fourier Transform, but unfortunately $\mathbf{F}_p$ usually does not contain appropriate roots of unity.

Instead we use **Bluestein's trick**:

$$\sum_{i=0}^{(p-3)/2} b_i g^{2ni} = g^{n^2} \sum_{i=0}^{(p-3)/2} (b_i g^{i^2}) g^{-(n-i)^2}.$$

This reduces the problem to a convolution of $\{b_i g^{i^2}\}_i$ with $\{g^{-i^2}\}_i$.

In other words: multiplying polynomials of degree $O(p)$ over $\mathbf{F}_p$!

So both the power series algorithm and Voronoi congruence algorithm reduce to multiplication of polynomials of degree $O(p)$ over $\mathbf{F}_p$.

How do we efficiently perform such a multiplication?

One option: lift to multiplication in $\mathbf{Z}[x]$.

For this, use some combination of floating-point FFTs and/or FFT modulo q for 'special' primes q (i.e. for which $\mathbf{F}_q$ contains suitable roots of unity).

Example: suppose $p \sim 2^{31}$.

Let $f, g \in \mathbf{Z}[x]$ with coefficients in $[0, p)$.

Then coefficients of fg have roughly $3 \times 31 = 93$ bits.

Floating-point only gives 53 bits of precision.

If we used 64-bit primes q_i, we would need two such primes.

This was the state of the art in Buhler–H. (2011) and previous work.

A different approach: consider again the DFT

$$\sum_{i=0}^{p-2} a_i g^{\ell i} \pmod{p},$$

where I have put $\ell = 2n - 1$.

Let us assume that $p = 2r + 1$ where r **is an odd prime**.

Of course not many p are of this form — but this is the simplest case.

Since r odd, it reduces to

$$\sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} a_i g^{\ell i} \pmod{p}.$$

Now we use **Rader's trick** — make *another* multiplicative rearrangement!

Note that $(\mathbf{Z}/(p-1)\mathbf{Z})^\times = (\mathbf{Z}/2\mathbf{Z})^\times \oplus (\mathbf{Z}/r\mathbf{Z})^\times \cong \mathbf{Z}/(r-1)\mathbf{Z}$.

Choose a generator $h \in (\mathbf{Z}/(p-1)\mathbf{Z})^\times$.

Make the substitution $i = h^{-s}$ and $\ell = h^t$.

Note that $i = r$ and $\ell = r$ are not covered by this substitution, since r is not invertible in $\mathbf{Z}/(p-1)\mathbf{Z}$.

For $\ell \neq r$ we get

$$\sum_{\substack{i=0 \\ i \text{ odd}}}^{p-2} a_i g^{\ell i} \qquad \Longrightarrow \qquad a_r g^{\ell r} + \sum_{s=0}^{r-1} a_{h^{-s}} g^{h^{t-s}}$$

The sum is a convolution of $\{a_{h^{-s}}\}_s$ and $\{g^{h^s}\}_s$.

And easy to check $a_r g^{\ell r} = 1$.

What's the point?

This is just another polynomial multiplication problem, of length $O(p)$, over $\mathbf{F}_p$.

However: the sequence $\{a_{h-s}\}_s$ has **very small coefficients**.

So when we lift multiplication to $\mathbf{Z}[x]$, the product coefficients have size $O(p^2)$ instead of $O(p^3)$.

In our example with $p \sim 2^{31}$, expect 62 bits instead of 93 bits.

So we can do it with a single prime q!

Example: $p = 59$, $r = 29$, $g = 2$, $h = 31$.

Take cyclic convolution of

$$(-1, +1, -1, -1, +1, -1, -1, +1, +1, +1, -1, -1, +1, -1,$$
$$-1, -1, -1, -1, -1, -1, -1, -1, -1, -1, +1, +1, +1, +1)$$

and

$$(2, 55, 43, 39, 13, 8, 54, 34, 24, 14, 40, 52, 10, 18,$$
$$30, 44, 11, 56, 50, 37, 47, 33, 32, 38, 31, 42, 6, 23),$$

and add 1. Over $\mathbf{Z}$ the result is

$$-(221, 255, 229, 259, 247, 273, 353, 301, 337, 297, 243, 297, 403, 295,$$
$$169, 111, 227, 321, 95, 125, 313, 249, 221, 269, 327, 315, 145, 163)$$

The entry 295 is zero modulo p, corresponding to $t = 13$, and thus the irregular index $h^t + 1 = 44 \pmod{p - 1}$.

Thank you!