About NFS@Home

NFS@Home is a research project that uses Internet-connected computers to do the lattice sieving step in the Number Field Sieve factorization of large integers. As a young school student, you gained your first experience at breaking an integer into prime factors, such as 15 = 3 * 5 or 35 = 5 * 7. NFS@Home is a continuation of that experience, only with integers that are hundreds of digits long. Most recent large factorizations have been done primarily by large clusters at universities. With NFS@Home you can participate in state-of-the-art factorizations simply by downloading and running a free program on your computer.

Integer factorization is interesting from both mathematical and practical perspectives. Mathematically, for instance, the calculation of multiplicative functions in number theory for a particular number require the factors of the number. Likewise, the integer factorization of particular numbers can aid in the proof that an associated number is prime. Practically, many public key algorithms, including the RSA algorithm, rely on the fact that the publicly available modulus cannot be factored. If it is factored, the private key can be easily calculated. Until quite recently, RSA-512, which uses a 512-bit modulus (155 digits), was commonly used but can now be easily broken.

The numbers what we are factoring are chosen from the Cunningham project. Started in 1925, it is one of the oldest continuously ongoing projects in computational number theory. The third edition of the book, published by the American Mathematical Society in 2002, is available as a free download. All results obtained since, including those of NFS@Home, are available on the

User of the day

MillliWillli

MillliWillli

News

New 15e number queued
A new C182 (the XYYXF number with the highest GNFS:SNFS difficulty ratio) is queued up on 15e; thanks to ChristianB for using two weeks of GPU time on his GeForce 750Ti to do the polynomial selection. 2340_742 will start linear algebra tomorrow. 15 Jul 2015, 20:52:50 UTC · Comment

10,359- factored
10,359- has been factored by GNFS. It is the product of 101- and 108-digit prime numbers. We still have lots of sieving to do for 6,490+. Thanks for your help! 4 Jul 2015, 3:35:35 UTC · Comment

16e status updated
The long neglected 16e status page has been updated with the ~~6~~ 7 factorizations completed so far this year. We will shortly have an 8th completed. Thanks for all of your contributions! 2 Jul 2015, 22:33:37 UTC · Comment

BOINC code upgrade
I'm working on transitioning the project's per-app credits from my custom code to the official BOINC code. Various credit- and badge-related displays may be a bit broken for a bit. Sorry for any inconvenience!

Edit: I think everything should be working now. Please let me know if you find anything broken by leaving a comment on this post. Thanks! 2 Jul 2015, 0:12:42 UTC · Comment

Cunningham project website.

NFS@Home is hosted at California State University Fullerton, and is supported in part by the National Science Foundation through XSEDE resources provided by the Texas Advanced Computing Center, the San Diego Supercomputer Center, the National Center for Supercomputing Applications, and Purdue University under grant number TG-DMS100027.

Join NFS@Home

- Read our rules and policies
- This project uses BOINC. If you're already running BOINC, select Attach to Project. If not, download BOINC.
- When prompted, select **NFS@Home** from the list of projects.
- If you're running a command-line or pre-5.0 version of BOINC, create an account first.
- If you have any problems, get help here.
- Detailed status of lasieved
- Detailed status of lasievee
- Server status

Returning participants

- Your account - view stats, modify preferences
- Teams - create or join a team
- Certificate
- Applications

Community

- Profiles
- User search
- Message boards
- Status of Numbers
- Statistics
- Languages
- Special contributions

193-digit GNFS coming atcha!
After five GPU-weeks of polynomial selection and a thousand CPU-hours of trial sieving, I've queued up a 193-digit GNFS from the aliquot-sequences project.

For this one I choose parameters to run through c5=1..10^7 in five GPU-weeks, which came out as stage-1 norm of 1e28 and stage-2 of 1e26. The best polynomial came from the first block, with c5=286440. Average yield (over Q=5e7*N .. 5e7*N+1e4 for N=1..8) is just slightly under 1, so I'm sieving 50M..500M to get a good number of relations.

There will be a 190-digit coming in about another three weeks when the polynomial selection's finished. 1 May 2015, 20:21:04 UTC · Comment

... more

News is available as an RSS feed


POWERED BY
BOINC


CALIFORNIA STATE UNIVERSITY
FULLERTON