1	~~2~~	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Figure 3.1 *Using the sieve of Eratosthenes to find the primes less than 100.*

$\pi(100) = 25$

x	$\pi(x)$	$x/\log x$	$\pi(x)/\frac{x}{\log x}$	$Li(x)$	$\pi(x)/Li(x)$
10^3	168	144.8	1.160	178	0.9438202
10^4	1229	1085.7	1.132	1246	0.9863563
10^5	9592	8685.9	1.104	9630	0.9960540
10^6	78498	72382.4	1.085	78628	0.9983466
10^7	664579	620420.7	1.071	664918	0.9998944
10^8	5761455	5428681.0	1.061	5762209	0.9998691
10^9	50847534	48254942.4	1.054	50849235	0.9999665
10^{10}	455052512	434294481.9	1.048	455055614	0.9999932
10^{11}	4118054813	3948131663.7	1.043	4118165401	0.9999731
10^{12}	37607912018	36191206825.3	1.039	37607950281	0.9999990
10^{13}	346065536839	334072678387.1	1.036	346065645810	0.9999997
10^{14}	3204941750802	3102103442166.0	1.033	3204942065692	0.9999999

Table 3.1 *Approximations to* $\pi(x)$.

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$$

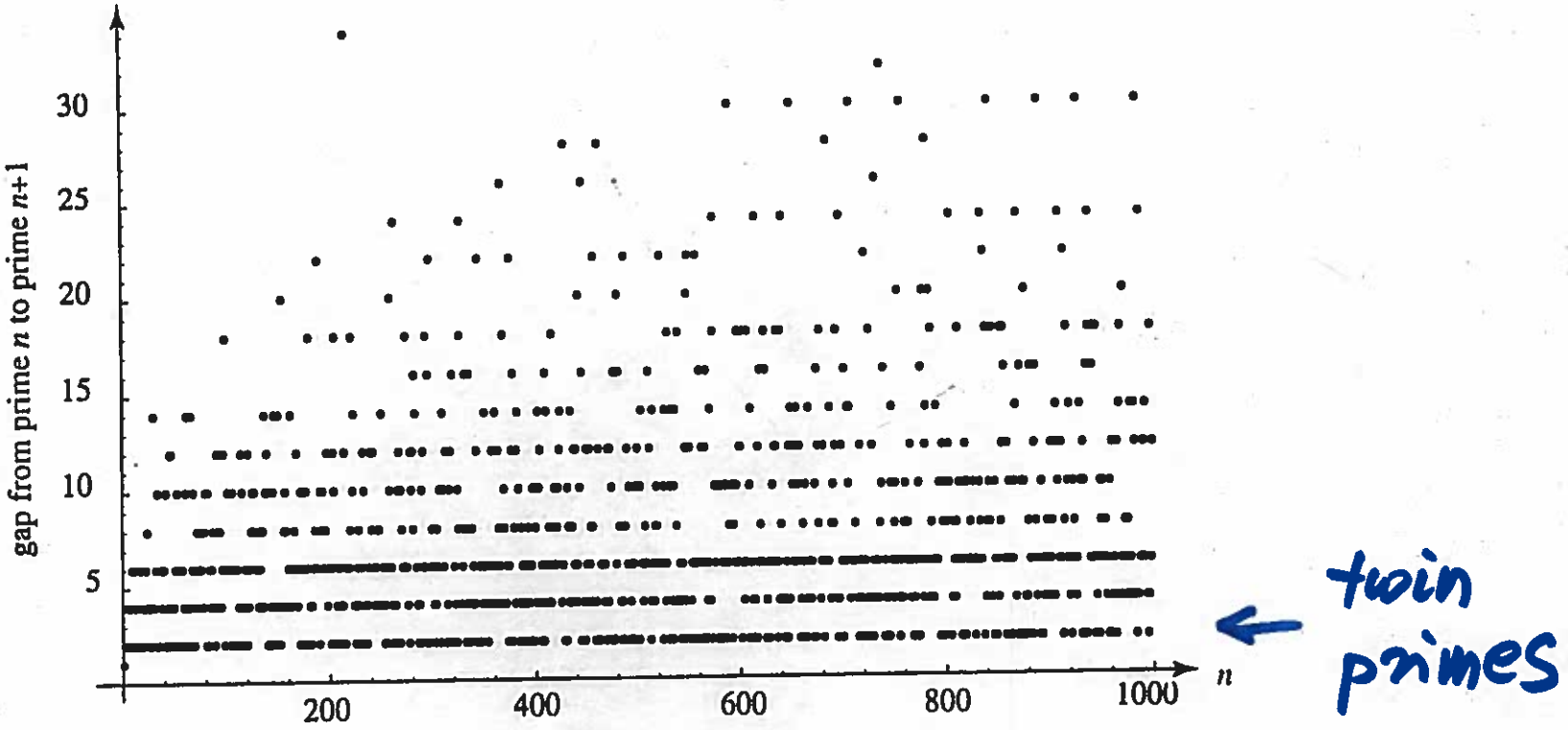


Figure 4.2 Gaps between successive primes.

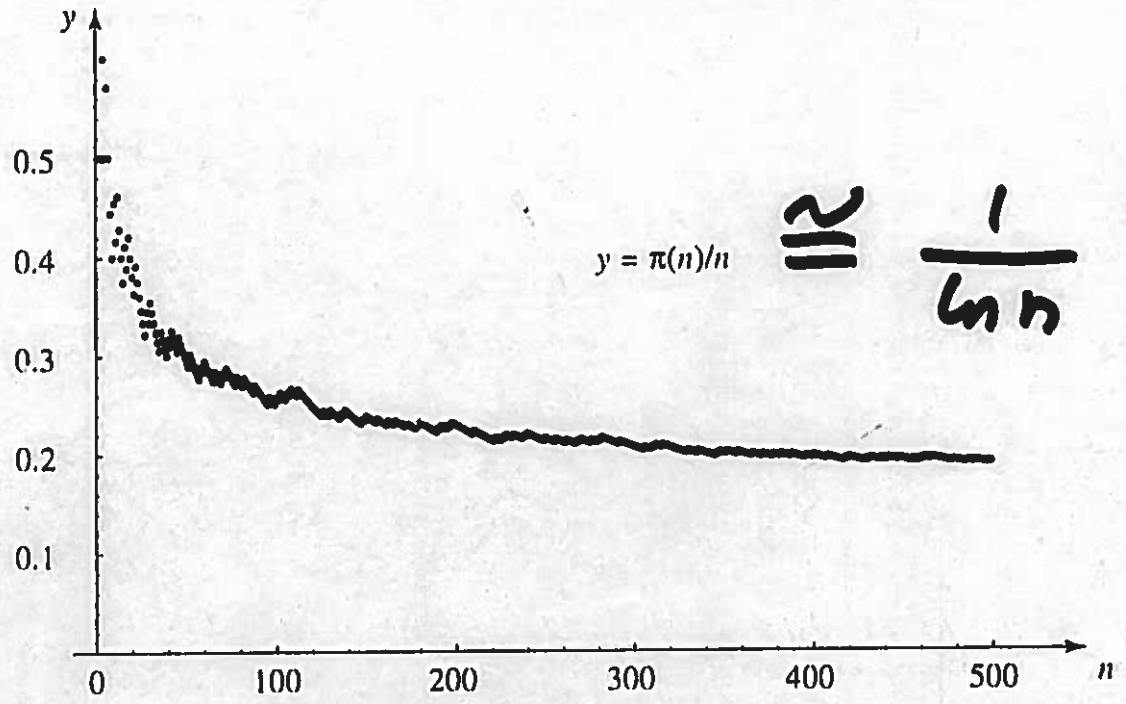


Figure 4.5 The density of primes as a function of n, $y = \pi(n)/n$.

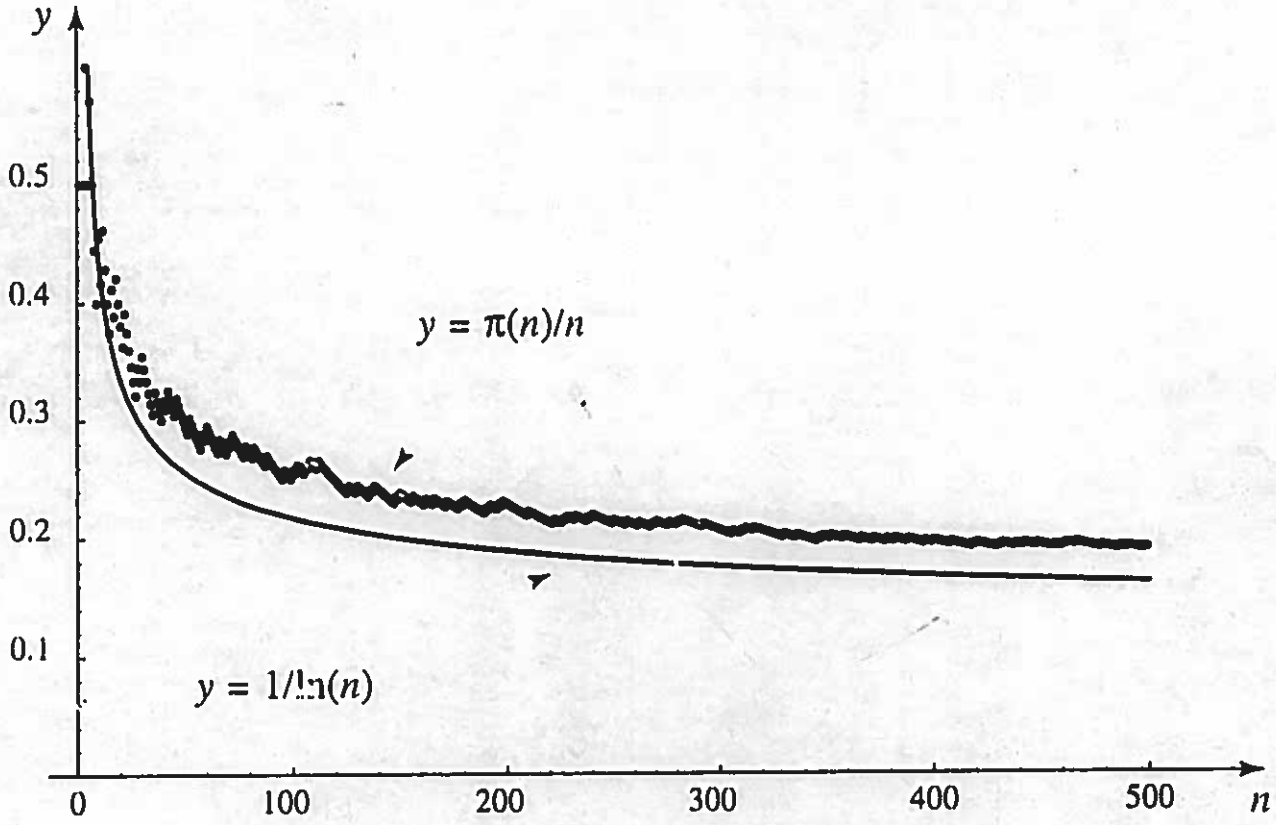


Figure 4.4 Graphs of $y = \pi(n)/n$ and $y = 1/\ln n$ superimposed.

$$\pi(n) \approx \frac{n}{\ln n}.$$

$e = 2.71828$

$\ln(10) = 2.306$

$\ln(2) = 0.693$

$$\pi(n) = \frac{n}{\ln n}$$

expected # of tries of Solovay-Strassen test before it generates a prime

100 digits $\ln(10^{100}) = 231$

1000 bits $\ln(2^{1000}) = 693$

or $\frac{1}{2}$ of that if no even tried ....

#	p	M_p	M_p digits	Discovered	Discoverer	Method used
1	2	3	1	c. 430 BC	Ancient Greek mathematicians[16]	
2	3	7	1	c. 430 BC	Ancient Greek mathematicians[16]	
3	5	31	2	c. 300 BC	Ancient Greek mathematicians[17]	
4	7	127	3	c. 300 BC	Ancient Greek mathematicians[17]	
5	13	8191	4	1456	Anonymous[18][19]	Trial division
6	17	131071	6	1588[20]	Pietro Cataldi	Trial division[21]
7	19	524287	6	1588	Pietro Cataldi	Trial division[22]
8	31	2147483647	10	1772	Leonhard Euler[23][24]	Enhanced trial division[25]
9	61	2305843009213693951	19	1883 November[26]	I. M. Pervushin	Lucas sequences
10	89	618970019642...137449562111	27	1911 June[27]	Ralph Ernest Powers	Lucas sequences
11	107	162259276829...578010288127	33	1914 June 1[28][29][30]	Ralph Ernest Powers[31]	Lucas sequences
12	127	170141183460...715884105727	39	1876 January 10[32]	Édouard Lucas	Lucas sequences
13	521	686479766013...291115057151	157	1952 January 30[33]	Raphael M. Robinson	LLT / SWAC
14	607	531137992816...219031728127	183	1952 January 30[33]	Raphael M. Robinson	LLT / SWAC
15	1,279	104079321946...703168729087	386	1952 June 25[34]	Raphael M. Robinson	LLT / SWAC
16	2,203	147597991521...686697771007	664	1952 October 7[35]	Raphael M. Robinson	LLT / SWAC

Great Internet Mersenne Prime Search

GIMPS

Finding World Record Primes Since 1996

Username
Password
Log In
Forgot password?

Home | Get Started | Current Progress | Account/Team Info | Reports | Manual Testing | More Information / Help | Donate — Make a donation

Welcome to GIMPS, the Great Internet Mersenne Prime Search

To join GIMPS, follow these instructions

Quick Links: Downloads | Stress Test | Known Primes | Progress Overview | Milestones | History

Today's Numbers	
Teams	848
Users	141,157
CPUs	1,159,380
TFLOP/s	295.055
GHz-Days	147,527

M(32582657) proven to be 44th Mersenne Prime

November 8, 2014 — In 2006, M(32582657) was discovered, and after 8 years GIMPS has finished checking and double-checking every smaller Mersenne number. With no new, smaller primes found, M(32582657) is officially the "44th Mersenne prime". Congratulations and thanks to all the GIMPS members that contributed their resources towards this milestone.

Prime95 version 28 released! Faster on Intel's latest CPUs!

June 1, 2014 — Version 28 is now available for download. The FFT assembly code has been optimized to use Intel's fused multiply-add instructions on Intel's Haswell CPUs (Core i3/i5/i7-4xxx models). Haswell users should see a decent performance increase. Sandy Bridge and Ivy Bridge users may also see a small speed boost due to some memory bandwidth optimizations. To upgrade, simply exit Prime95, download the new version, and unzip the new version replacing the old version.

New Assignment and Recycling Rules

February 2014 — Since 2008, GIMPS has given users one year to complete assignments. This rule has not been enforced. This has held up completing milestones as some assignments did not complete even after several years.

During February 2014, new assignment and recycling policies were put in place to help GIMPS make steady progress on milestones by detecting assignments that are proceeding extremely slowly or not at all.

This affects users in two ways:

- When they occasionally become available, if you want to test the smallest exponents you'll need to sign up on the assignment rules page and be aware of the shorter timeline for returning results.
- Your computers that are proven producers will have 8 or 9 months to complete assignments. Your slower computers and computers with a limited track record will still have a full year to complete their assignments.

Great Internet Mersenne Prime Search

GIMPS

Finding World Record Primes Since 1996

Username Password Log In Forgot password?

Home | Get Started | Current Progress | Account/Team Info | Reports | Manual Testing | More Information / Help | Donate — Make a donation

PrimeNet Activity Summary 2015-11-16 15:00 UTC

Stats updated in the first minutes of every hour

Aggregate Computing Power

Today, last 24 hours		Week, last 7 days		Month, last 30 days	
Potential TFLOP/sec	Actual TFLOP/sec	Potential TFLOP/sec	Actual TFLOP/sec	Potential TFLOP/sec	Actual TFLOP/sec
175.526	295.055	332.283	242.308	706.981	264.457
Power	GHz-Days	Power	GHz-Days	Power	GHz-Days
168%	147527	72%	848078	37%	3966855

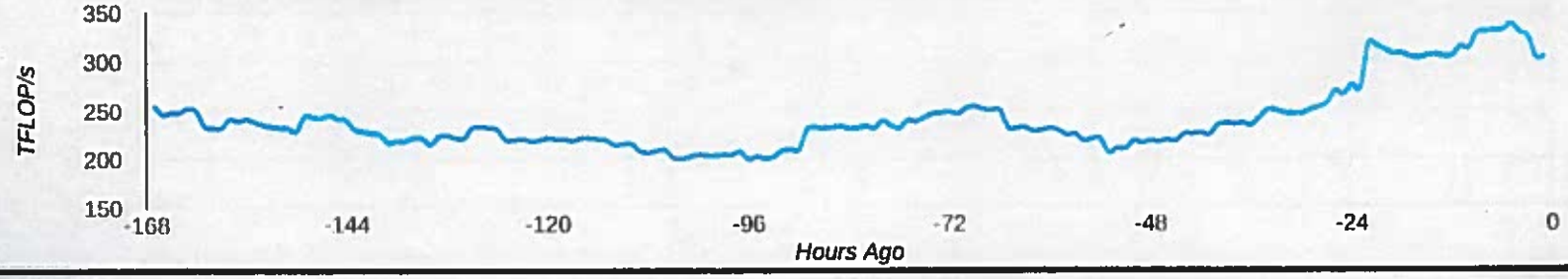
Resources Registered

teams	848
user IDs	141157
computers	1159380
work units	559672

Recently Active and Work Done

Resource	24 hours	7 days	30 days
user IDs	1874	2596	3547
computers	6908	12374	24727
work units	80459	421950	1783706

Trillions of calculations per second (TFLOP/s), CPU results last 7 days



Exponent Status Distribution

Exponent Range Start	Count	P	Composite F	Composite LL-D	Status Unproven LL	Status Unproven LLERR	Status Unproven NO-LL	Assigned ECM	Assigned P-1	Assigned LL	Assigned LL-D	Available ECM	Available P-1	Available LL	Available LL-D
0	78498	33	61666	16799				897				16784			
1000000	70435	2	50557	19876				197				19876			
2000000	67883	1	46500	21382				283				21382			
3000000	66330	1	44345	21984				164	182			21802			

Users testing 100 million digit numbers are not affected by these new rules. Assignments made prior to March 1, 2014 will be given a year, as promised, to complete (plus a grace period if the assignment is close to complete).

M(30402457) proven to be 43rd Mersenne Prime

February 23, 2014 — More than 8 years after discovering M(30402457), GIMPS has finished checking and double-checking every smaller Mersenne number. With no new primes found that are smaller than M(30402457), the "43rd known Mersenne prime" can now be called the "43rd Mersenne prime". Congratulations and thanks to all the GIMPS members that perform this somewhat less glamorous double-checking work.

Largest Known Prime, 48th Known Mersenne Prime Found!!

January 25th, 2013 — Prolific GIMPS contributor Dr. Curtis Cooper discovered the 48th known Mersenne prime, $2^{57,885,161}-1$, a 17,425,170 digit number. This find shatters the previous record prime number of 12,978,189 digits, also a GIMPS prime, discovered over 4 years ago. The discovery is eligible for a $3,000 GIMPS research discovery award.

Dr. Cooper is a professor at the University of Central Missouri. This is the third record prime for Dr. Cooper and his University. Their first record prime was discovered in 2005, eclipsed by their second record in 2006. Computers at UCLA broke that record in 2008. UCLA held the record until Dr. Cooper and the University of Central Missouri reclaimed the world record with this discovery.

While Dr. Cooper's computer found the record prime, the discovery would not have been possible without all the GIMPS volunteers that sifted through numerous non-prime candidates. GIMPS founder George Woltman and PrimeNet creator Scott Kurowski thank and congratulate all the GIMPS members that made this discovery possible.

Mersenne primes are extremely rare, only 48 are known. GIMPS, founded in 1996, has discovered the last 14 Mersenne primes. Mersenne primes were named for the French monk Marin Mersenne, who studied these numbers more than 350 years ago. Chris Caldwell maintains an authoritative web site on the history of Mersenne primes as well as the largest known primes.

The primality proof took 39 days of non-stop computing on one of the University of Central Missouri's PCs. To establish there were no errors during the proof, the new prime was independently verified using different programs running on different hardware. Jerry Hallett verified the prime using CUDALucas running on a NVidia GPU in 3.6 days. Dr. Jeff Gilchrist verified the find using the standard GIMPS software on an Intel i7 CPU in 4.5 days. Finally, Serge Batalov ran Ernst Mayer's MLucas software on a 32-core server in 6 days (resource donated by Novartis IT group) to verify the new prime.

You can read a little more in the short press release.

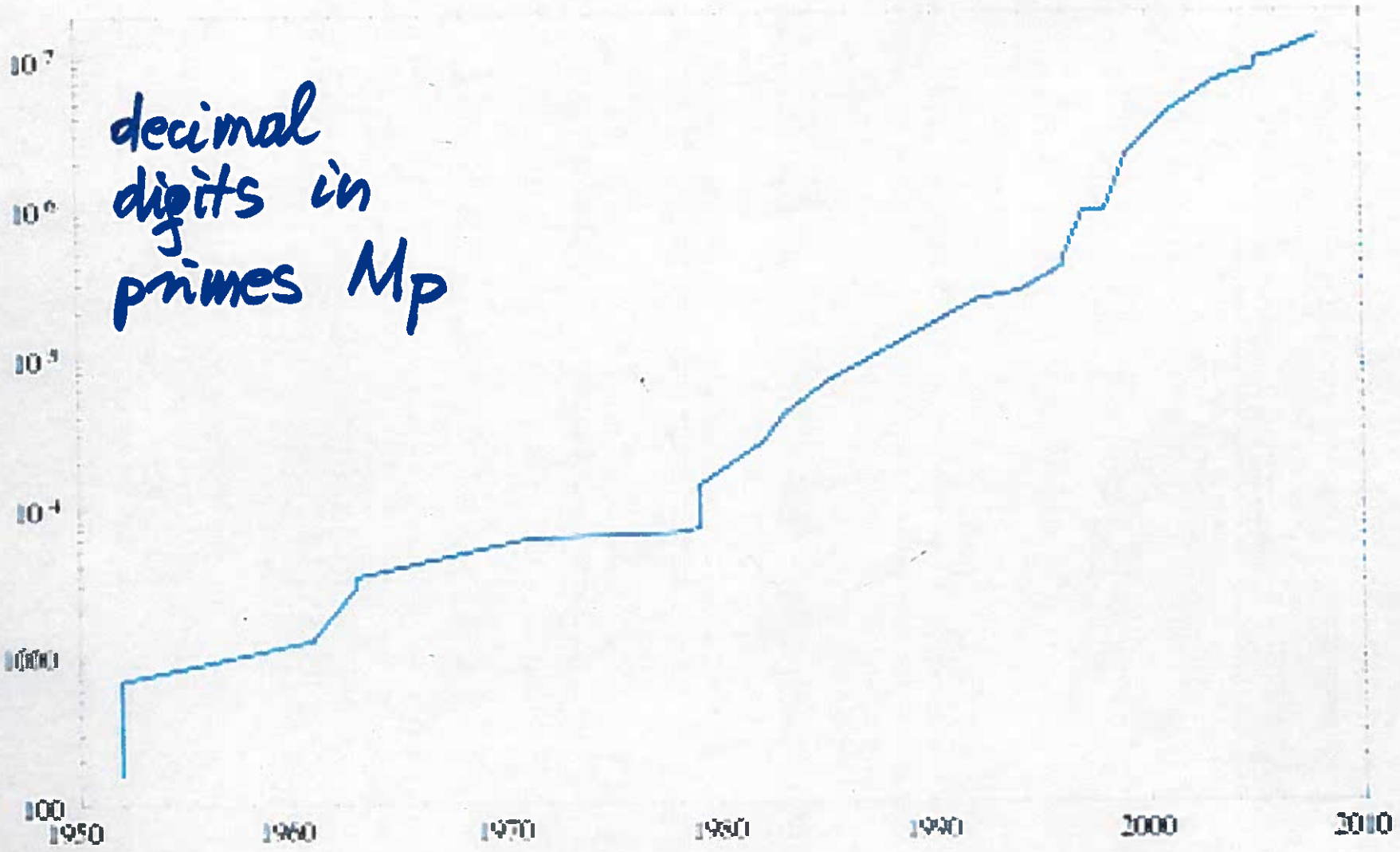
M(25964951) proven to be 42nd Mersenne Prime

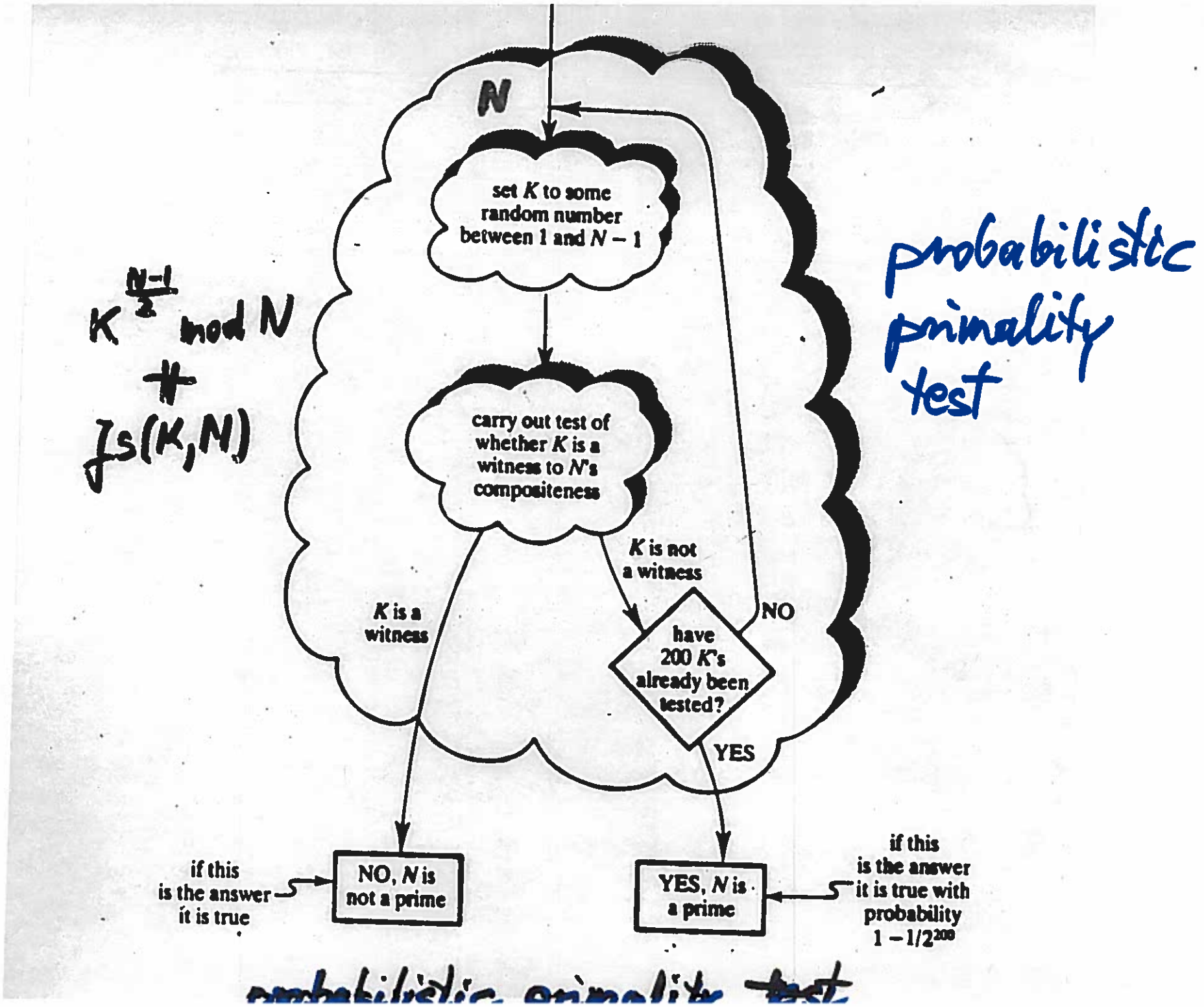
December 20, 2012 — One year after proving the 41st Mersenne prime, GIMPS finished double-checking every smaller Mersenne number than M(25964951) -- proving that this prime is indeed the 42nd Mersenne prime. There are 47 known Mersenne primes. Mersenne primes are sometimes discovered out-of-order. It is not yet known if there is an undiscovered Mersenne prime between M(25964951) and the next largest known Mersenne prime, M(30402457). Here is a list of all GIMPS milestones and our progress toward future ones. Congratulations and thanks to all the GIMPS members that contributed to this important double-checking work.

Prime95 version 27 released! Faster on Intel's newer CPUs!

May 15, 2012 — You may download version 27 now. The FFT assembly code has been rewritten for better speed on Intel's newer CPUs supporting AVX instructions. Sandy Bridge and Ivy Bridge CPUs (Core i3/i5/i7-2xxx and 3xxx models) should see a huge performance increase. To upgrade, simply exit Prime95,

#	p	Factorization of M_p
1	11	23 × 89
2	23	47 × 178481
3	29	233 × 1103 × 2089
4	37	223 × 616318177
5	41	13367 × 164511353
6	43	431 × 9719 × 2099863
7	47	2351 × 4513 × 13264529
8	53	6361 × 69431 × 20394401
9	59	179951 × 3203431780337 (13 digits)
10	67	193707721 × 761838257287 (12 digits)
11	71	228479 × 48544121 × 212885833
12	73	439 × 2298041 × 9361973132609 (13 digits)
13	79	2687 × 202029703 × 1113491139767 (13 digits)
14	83	167 × 57912614113275649087721 (23 digits)
15	97	11447 × 13842607235828485645766393 (26 digits)
16	101	7432339208719 (13 digits) × 341117531003194129 (18 digits)
17	103	2550183799 × 3976656429941438590393 (22 digits)
18	109	745988807 × 870035986098720987332873 (24 digits)
19	113	3391 × 23279 × 65993 × 1868569 × 1066818132868207 (16 digits)
20	131	263 × 1035079443105516238671861923746823456 9 (38 digits)
...	...	...
23	149	86656268566282183151 (20 digits) × 823510933669084672398616 1 (25 digits)
...	...	...
43	257	535006138814359 (15 digits) × 1155685395246619182673033 (25 digits) × 3745505985018109365817766300963131813 93 (39 digits)
...	...	...


decimal
digits in
primes Mp
10^7
10^6
10^5
10^4
1000
100
1950
1960
1970
1980
1990
2000
2010



$K^{\frac{N-1}{2}} \bmod N$

$+$

$Js(K,N)$

probabilistic primality test

probabilistic primality test

FIGURE 4.7
The Solovay-Strassen primality test for an odd integer n

1. choose a random integer a, $1 \leq a \leq n-1$
2. if $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$ then
   answer "n is prime"
   else
   answer "n is composite"

Stinson, page 188

Algorithm 5.7: MILLER-RABIN(n)

write $n - 1 = 2^k m$, where m is odd
choose a random integer a, $1 \leq a \leq n - 1$
$b \leftarrow a^m \bmod n$
if $b \equiv 1 \pmod{n}$
  then return ("n is prime")
for $i \leftarrow 0$ **to** $k - 1$
  do { **if** $b \equiv -1 \pmod{n}$
    then return ("n is prime")
    else $b \leftarrow b^2 \bmod n$
return ("n is composite")

$s = 1$

MR(a, n)

$Pr(\text{error}) \leq \frac{1}{4}$

AKS algorithm people, 2002

Nitin Saxena

Neeraj Kayal

Manindra Agrawal

factorization cost

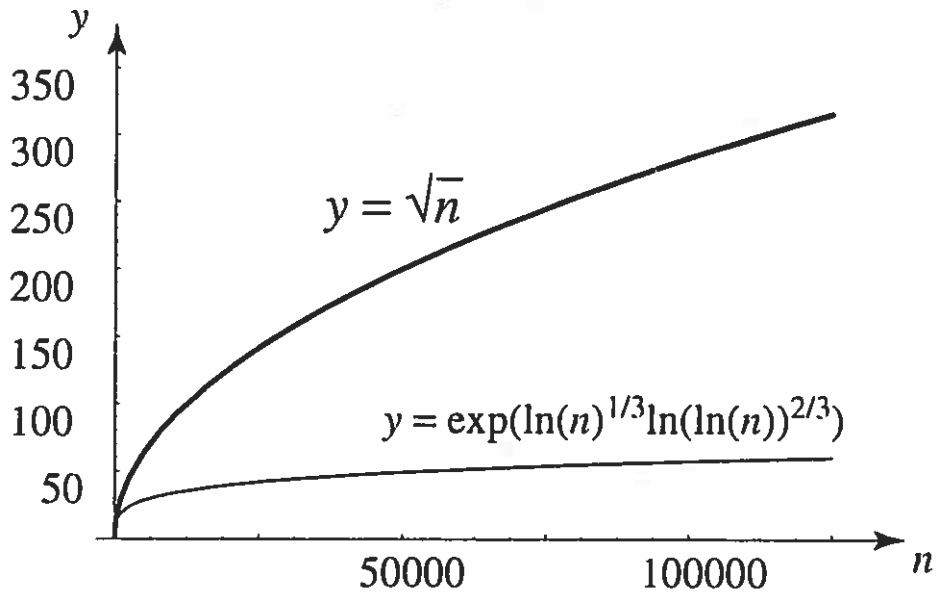


Figure 4.5 Comparing the computational expense of trial division (upper curve) with the number field sieve (lower curve).

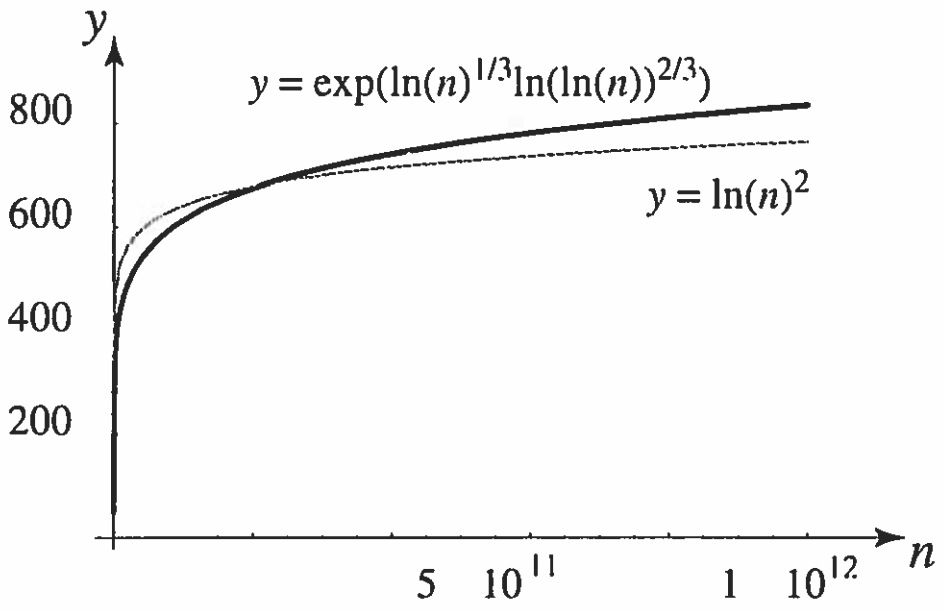


Figure 4.6 Comparing the computational expense of the number field sieve (dark curve) with that of a putative polynomial time algorithm (light curve).

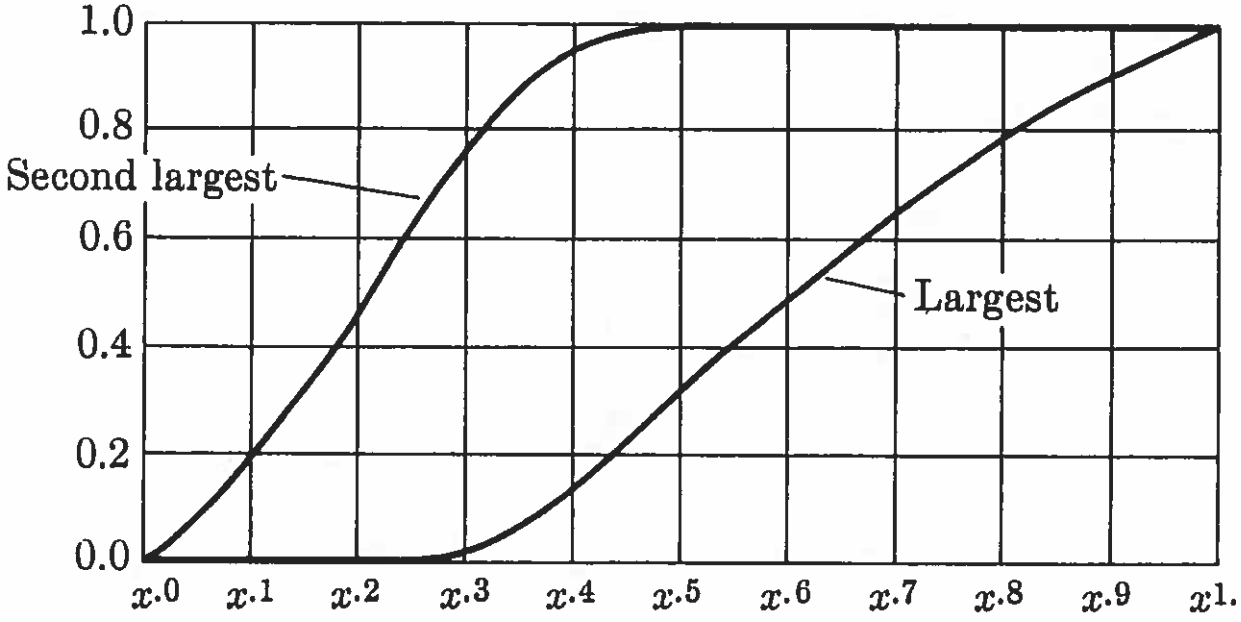


Fig. 11. Probability distribution functions for the two largest prime factors of a random integer $\leq x$.

Project/URL	Research Base	Goal
Mersenne Prime Search www.mersenne.org	Worldwide	Identify enormous prime numbers
SETI@home setiathome.ssl.berkeley.edu	UC Berkeley	Find extraterrestrial intelligence
Folding@home folding.stanford.edu	Stanford	Predict how proteins fold
ClimatePrediction.net climateprediction.net	Oxford	Test models of climate change
LHC@home lhcathome.cern.ch	CERN	Model particle orbits in accelerator
Einstein@home einstein.phys.uwm.edu	U.S. and Germany	Identify gravitational waves
Cancer Research Project www.grid.org/projects/cancer	NCI and Oxford	Search for candidate drugs against cancer
Lifemapper www.lifemapper.org	University of Kansas	Map global distribution of species