Peter Lawrence Montgomery

25 September 1947 – 18 February 2020

Peter Lawrence Montgomery

Born on September 25, 1947 in San Francisco, CA

1967.   Among the five highest ranking participants in the
               William Lowell Putnam Mathematical competition

1969.   BA in Mathematics (UC Berkeley)

1971.   MA in Mathematics (UC Berkeley)

1972-1982.   Scientific and system programming at
               System Development Corporation (SDC), Huntsville, Alabama

1982-1989.   Transferred to SDC (later renamed Unisys) in Santa Monica, California

1992.   PhD in mathematics under supervision of David G. Cantor
               Thesis: An FFT extension of the elliptic curve method of factorization

1998.   Joined Microsoft Research in Redmond, WA.

2014.   Retirement.

Died February 18, 2020 in Pong, Thailand
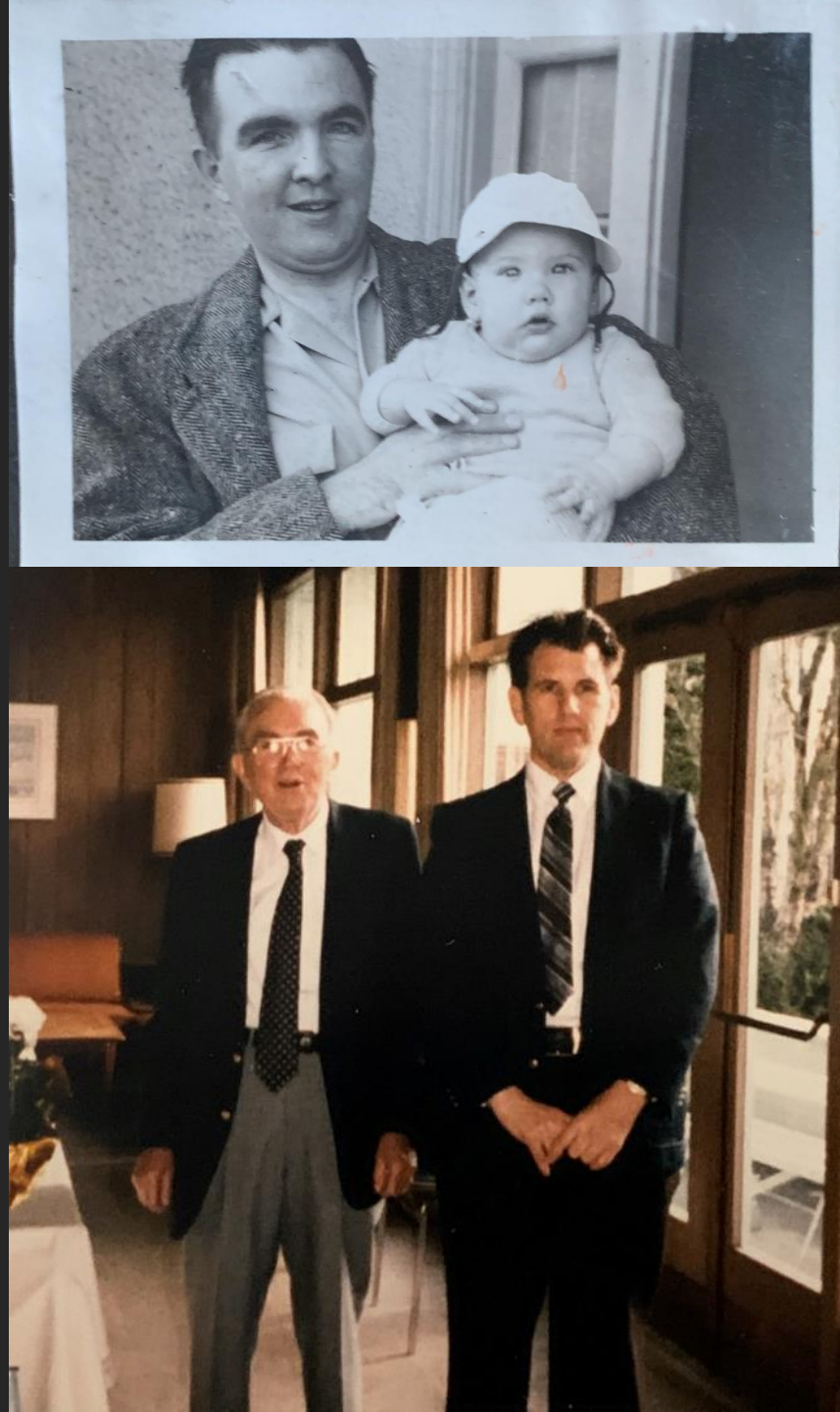
Most widely used contributions

Have you
- visited a web page,
- performed an electronic payment,
- used a messaging application

today?

If so, then you have probably used one of the mathematical techniques proposed by and named after Peter Montgomery.

- Montgomery multiplication
  Main approach used in RSA
  → virtually all HTTPS certificates use RSA for signatures
- Montgomery curves
  Example: Curve25519 used in Signal, WhatsApp, TLS, etc
- Montgomery ladder
  Essential technique to harden (against side-channel attacks) ECC implementations. Used in billions of payments and transit products.

See for more info: www.joppebos.com/montgomery

TOPICS IN

COMPUTATIONAL NUMBER THEORY

INSPIRED BY

PETER L. MONTGOMERY
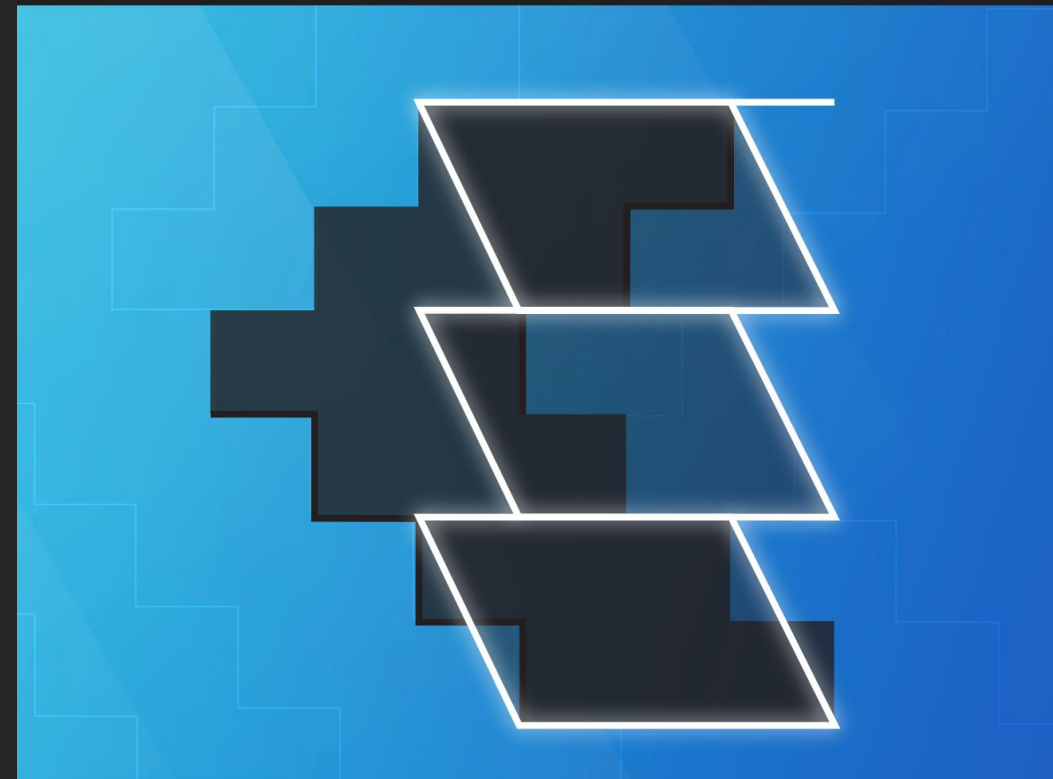
CAMBRIDGE

JOPPE W. BOS AND ARJEN K. LENSTRA

Integer Factorization Contributions

General Purpose Factorization algorithms
Run-time depends on the size of the input integer
- Multiple Polynomial Quadratic Sieve
- Number Field Sieve
  - Polynomial Selection
  - Line Sieving
  - Matrix step (block Lanczos)
  - Square root

Special Purpose Factorization algorithms
Run-time depends mainly on the size of the unknown prime divisor
- FFT approach for Stage 2 algorithms for Pollard p-1 and ECM (PhD topic)
- Speeding-up ECM
  - Montgomery curves
  - Montgomery ladder

Selected Computational records
2010. ECM factorization record
      (73-digit factor of $2^{1181} - 1$)
2010. Integer factorization record: RSA-768
2009. 112-bit ECDLP record on cluster of PS3s
2000. Integer factorization record: RSA-512
1999. Integer factorization record: RSA-140

ECM – Then and Now

"Other people have a work life and a personal life.
I have a work life and a research life."

GRADE REQUEST CARD

Name of Student: Peter Montgomery

Department and Course Number: Math 214 A

Final Examination Grade: A+

Final Grade in Course: A+

This acknowledges receipt of a solution to problem 5785 in the March, 1971, issue of the American Mathematical Monthly.
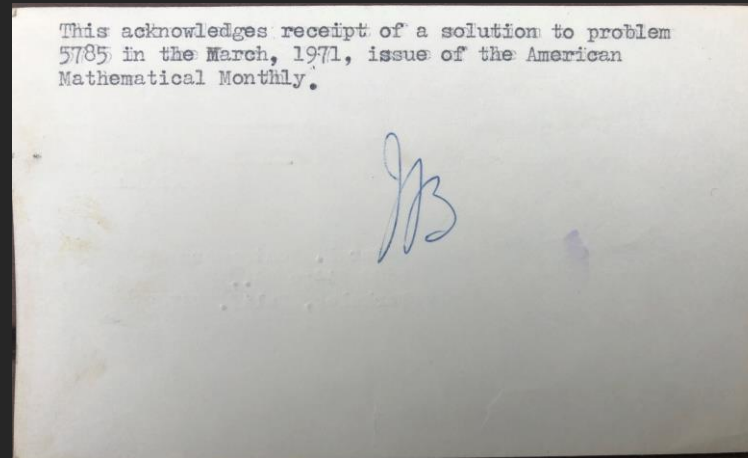
"Peter's passion for his research, which aligned with his work life, was why his work was all consuming. He truly loved doing Mathematics.

It was in the mathematical community that Peter truly found his place, among people who shared his passions, and didn't expect him to conform to arbitrary standards. This community was more than a career for him, it was where he belonged." (Dan Shumow)
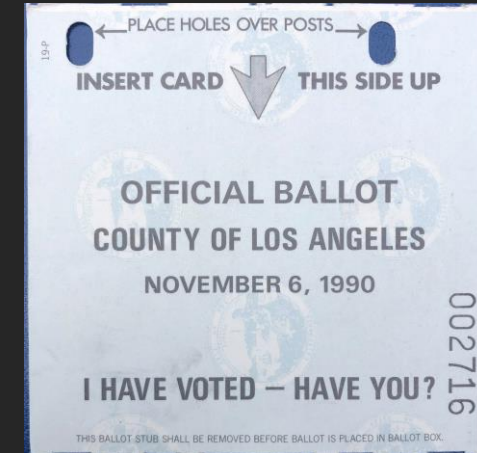
Mathematics of Computation
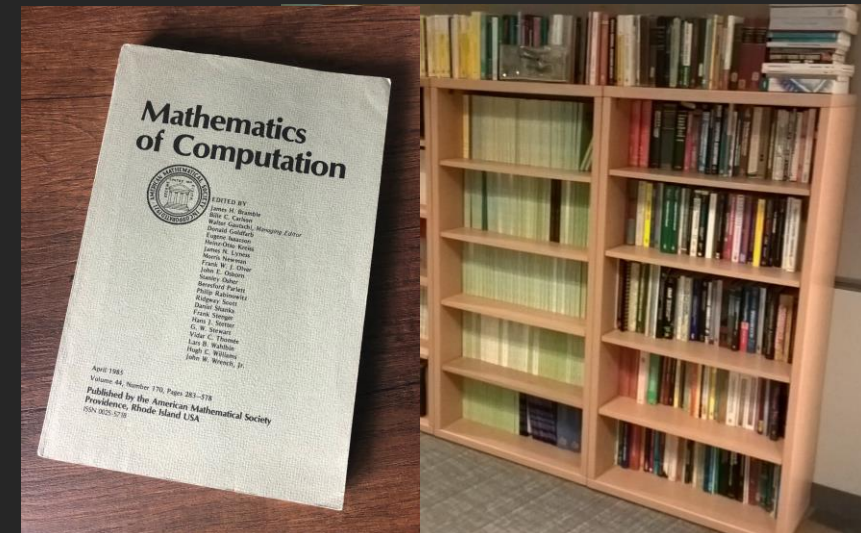
WHERE'S MY LANE?

"The environmental movement blossomed while I was at Berkeley, and I vowed in 1972 never to drive again."

"But Huntsville lacked sidewalks between home and work. For one year, I walked with large placards "WE NEED SIDEWALKS" and "WHERE'S MY LANE", until the City Council voted to install sidewalks near schools and to fund bike lanes and paths."

CITY OF SAN RAFAEL
PRESENTS THIS
RESOLUTION OF APPRECIATION
TO

PETER MONTGOMERY

WHEREAS, in January, 2001 the City Council directed a Shuttle Bus Feasibility Study; and

WHEREAS, staff was directed to form a Shuttle Study Advisory Group to help develop goals and objectives and to oversee the study process; and

WHEREAS, in April, 2001 Peter was invited by the Mayor to participate, as a key stakeholder, in the Shuttle Study Advisory Group; and

WHEREAS, Peter was a valuable participant and provided the committee with insight, experience and expertise, and helped to direct the study to benefit everyone in San Rafael; and

WHEREAS, the Shuttle Bus Feasibility Study will be used to implement future circulation and parking improvements in San Rafael.

NOW, THEREFORE, BE IT RESOLVED that the Mayor and City Council hereby express sincere appreciation and gratitude to Peter Montgomery for his substantial contribution of time and effort to complete the shuttle study that will serve to guide and assist with future public transportation projects, and for his commitment to the betterment of the San Rafael community.

ATTESTED BY MY HAND THIS 18th DAY OF March, 2002

← PLACE HOLES OVER POSTS →
INSERT CARD ↓ THIS SIDE UP

OFFICIAL BALLOT
COUNTY OF LOS ANGELES
NOVEMBER 6, 1990
I HAVE VOTED — HAVE YOU?

THIS BALLOT STUB SHALL BE REMOVED BEFORE BALLOT IS PLACED IN BALLOT BOX.

002716

"He loved children and was very happy helping me watch them during the excursion at the Banff conference. He thought that all of their thoughts and requests were perfectly reasonable and wanted to accommodate all of them."
(Kristin Lauter)
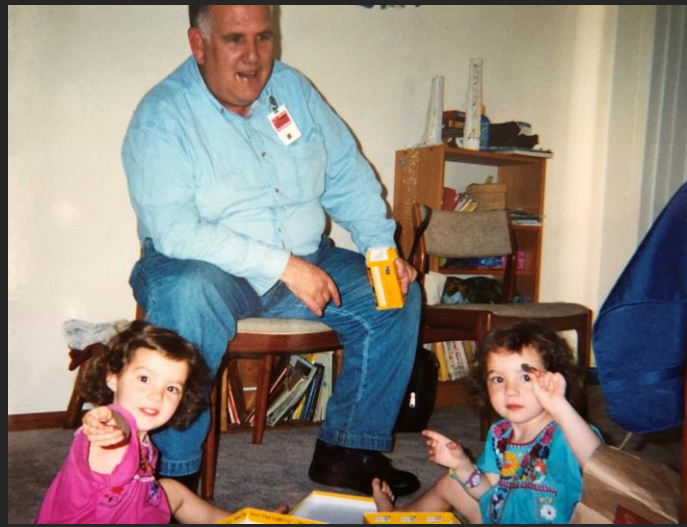
(With Kristin Lauter's twin daughters Joyce and Josephine, 2003)

(Banff, 2003)

"Peter adored my children - his niece Heather, and his nephew Page...

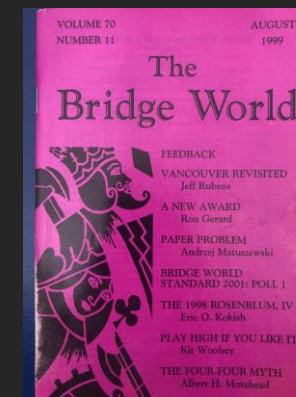He would take the kids on long walks around town until he wore them out...
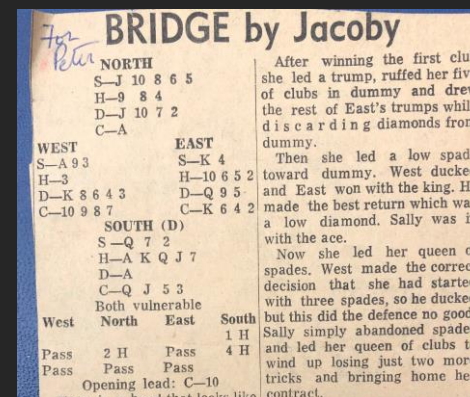
One thing he liked to do was name all the states that had a particular letter in their names.
(Betty Montgomery, sister-in-law)

"He was brilliant in pulling out some contracts with just stellar play of the hands - he always remembered every card played and would have made a fortune in Vegas as a card counter but had zero interest in that."
(Richard Montgomery, brother)

"It was difficult to play bridge with him because he would memorize each card as it was played and calculate who had what cards."
(Betty Montgomery, sister-in-law)

"He knew I liked bridge, so for many years he would cut out the bridge column from the newspaper on a daily or weekly basis and leave it on my desk in the morning so we could discuss it at lunch."
(Kristin Lauter)
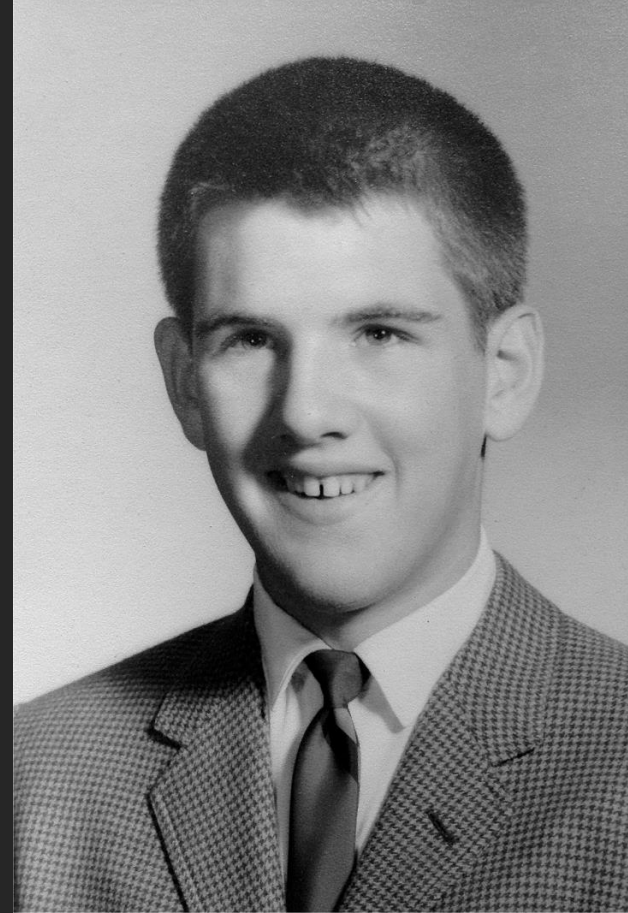
"If you took the time to get to know him, you would discover one of the keenest minds imaginable, and one of the kindest people you could ever meet." (Betty Montgomery, sister-in-law)

Peter Lawrence Montgomery

25 September 1947 – 18 February 2020

"Yet in spite of everything that limited him, Peter did what all of us hope to do, what all of us wish we could say at the end of our days. Peter made a difference."
(Betty Montgomery, sister-in-law)