What if Gauss had had a computer?

Paul Zimmermann, INRIA, Nancy, France

Celebrating 75 Years of Mathematics of Computation, ICERM, Brown University, Providence, November 1st, 2018
Carl Friedrich Gauss, Werke, Volume 2, 1863, pages 477-502:

TAFEL

ZUR

CYKLOTECHNIE.
What if Gauss had had a computer?
What if Gauss had had a computer?
\[ \frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239} \quad \text{(Machin, 1706)} \]

\[ \begin{align*}
\text{Gauss, 1.} & = 12 \left( \frac{1}{18} \right) + 8 \left( \frac{1}{57} \right) - 5 \left( \frac{1}{239} \right) \\
\text{Gauss, 2.} & = 12 \left( \frac{1}{38} \right) + 20 \left( \frac{1}{57} \right) + 7 \left( \frac{1}{239} \right) + 24 \left( \frac{1}{268} \right) 
\end{align*} \]

\[ \frac{\pi}{4} = 12 \arctan \frac{1}{18} + 8 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239} \quad \text{(Gauss, 1863)} \]

\[ \frac{\pi}{4} = 12 \arctan \frac{1}{38} + 20 \arctan \frac{1}{57} + 7 \arctan \frac{1}{239} + 24 \arctan \frac{1}{268} \quad \text{(Gauss, 1863)} \]
Plan of the talk

- how such identities can be verified
- how they can be (re)discovered
- by hand and using modern computational mathematics tools
What if Gauss had had a computer?

\[
\text{sage: } a=4594; \text{ factor}(a^2 + 1) \\
13 \times 17 \times 29 \times 37 \times 89
\]
sage: factor(14033378718^2 + 1)
5^2 * 13 * 17^2 * 61^4 * 73^2 * 157 * 181

Even Gauss made errors...
sage: [a for a in [1..10^4] if largest_prime(a^2+1) == 5]
[2, 3, 7]
sage: [a for a in [1..10^4] if largest_prime(a^2+1) == 13]
[5, 8, 18, 57, 239]
sage: [a for a in [1..10^4] if largest_prime(a^2+1) == 109]
[33, 76, 142, 251, 294, 360, 512, 621, 905, 948, 1057, 1123, 1929, 2801, 3521, 3957, 5701, 6943, 8578, 9298]

What if Gauss had had a computer?
<table>
<thead>
<tr>
<th>Author</th>
<th>Formula</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machin</td>
<td>((1) = 4(5) - (239))</td>
<td>auch Clausen</td>
</tr>
<tr>
<td>Euler</td>
<td>((2) + (3))</td>
<td>(\text{Euler à Goldbach 1746 Mai 28})</td>
</tr>
<tr>
<td>Vega</td>
<td>(5(7) + \frac{79}{3})</td>
<td>(\text{Vega Thesaurus logar. p. 633})</td>
</tr>
<tr>
<td>Vega</td>
<td>(3(3) + (7))</td>
<td>auch Clausen (\text{Astr. Nachr. B. 25. S. 209})</td>
</tr>
<tr>
<td>Rutherford</td>
<td>(4(5) - (70) + (99))</td>
<td>(\text{Philos. Trans. 1841. p. 283})</td>
</tr>
<tr>
<td>Dase</td>
<td>((2) + (5) + (8))</td>
<td>(\text{Crelle Journal. B. 27. S. 198})</td>
</tr>
<tr>
<td>Gauss 1.</td>
<td>(12(18) + 8(57) - 5(239))</td>
<td></td>
</tr>
<tr>
<td>Gauss 2.</td>
<td>(12(38) + 20(57) + 7(239) + 24(268))</td>
<td></td>
</tr>
</tbody>
</table>

Notation: \((n)\) or \([n]\) denotes \(\arctan \frac{1}{n}\).
Measure of an arc-tangent identity

Lehmer proposes in 1938 the following measure. For example, Machin’s formula

\[
\frac{\pi}{4} = 4\arctan\frac{1}{5} - \arctan\frac{1}{239}
\]

has measure

\[
\frac{1}{\log_{10} 5} + \frac{1}{\log_{10} 239} \approx 1.8511
\]

A formula with measure say 2 needs two terms of the arc-tangent series to get one digit of \(\pi\):

\[
\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} \ldots
\]
Machin (1706, measure 1.8511):

\[ \frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239} \]

Gauss (1863, measure 1.7866):

\[ \frac{\pi}{4} = 12 \arctan \frac{1}{18} + 8 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239} \]

Gauss (1863, measure 2.0348):

\[ \frac{\pi}{4} = 12 \arctan \frac{1}{38} + 20 \arctan \frac{1}{57} + 7 \arctan \frac{1}{239} + 24 \arctan \frac{1}{268} \]
Why is the arc-tangent series so popular?

\[
\arctan \frac{1}{n} = \frac{1}{n} - \frac{1}{3n^3} + \frac{1}{5n^5} - \cdots
\]

\[
10^{15} \arctan \frac{1}{239} \approx \frac{10^{15}}{239} - \frac{10^{15}}{3 \cdot 239^3} + \frac{10^{15}}{5 \cdot 239^5}
\]

\[
\left\lfloor \frac{10^{15}}{239} \right\rfloor = 4184100418410
\]

\[
\frac{4184100418410}{239^2} = 73249775, \quad \frac{73249775}{3} = 24416591
\]

\[
\frac{73249775}{239^2} = 1282, \quad \frac{1282}{5} = 256
\]

\[
10^{15} \arctan \frac{1}{239} \approx 4184100418410 - 24416591 + 256 = 4184076002075
\]

What if Gauss had had a computer?
2-term identities

\[
\frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239} \quad \text{(Machin, 1706, measure 1.8511)}
\]

\[
\frac{\pi}{4} = 2 \arctan \frac{1}{3} + \arctan \frac{1}{7} \quad \text{(Machin, 1706, measure 3.2792)}
\]

\[
\frac{\pi}{4} = 2 \arctan \frac{1}{2} - \arctan \frac{1}{7} \quad \text{(Machin, 1706, measure 4.5052)}
\]

\[
\frac{\pi}{4} = \arctan \frac{1}{2} + \arctan \frac{1}{3} \quad \text{(Machin, 1706, measure 5.4178)}
\]

Störmer proved in 1899 these are the only ones of the form 
\[k \frac{\pi}{4} = m \arctan(1/x) + n \arctan(1/y).\]
3-term identities

The one with best measure (with numerators 1) is due to Gauss (1863, measure 1.7866):

$$\frac{\pi}{4} = 12 \arctan \frac{1}{18} + 8 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239}$$

Störmer found 103 3-term identities in 1896, Wrench found two more in 1938, and Chien-lih a third one in 1993. Their exact number remains an open question.
The one with best measure (with numerators 1) is due to Störmer (1896, measure 1.5860):

\[
\frac{\pi}{4} = 44 \arctan \frac{1}{57} + 7 \arctan \frac{1}{239} - 12 \arctan \frac{1}{682} + 24 \arctan \frac{1}{12943}
\]

It was used by Kanada et al. in 2002 to compute 1,241,100,000,000 digits of \(\pi\).

The second best was found by Escott in 1896 (measure 1.6344), the third one by Arndt in 1993 (1.7108).
Computation of $\pi$

1962: Shanks and Wrench compute 100,265 decimal digits of $\pi$ using Störmer’s formula (1896, measure 2.0973):

$$\frac{\pi}{4} = 6 \arctan \frac{1}{8} + 2 \arctan \frac{1}{57} + \arctan \frac{1}{239}$$

The verification was done with Gauss’ formula:

$$\frac{\pi}{4} = 12 \arctan \frac{1}{18} + 8 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239}$$

The first check did agree only to 70,695 digits, due to an error in the computation of $6 \arctan(1/8)$!

This was published in volume 16 of Mathematics of Computation. Pages 80-99 of the paper give the 100,000 digits.

1973: Guilloud and Boyer compute 1,001,250 digits using the same formulae.

What if Gauss had had a computer?
2002: Kanada et al. compute 1,241,100,000,000 digits using the self-checking pair

\[
\frac{\pi}{4} = 44 \arctan \frac{1}{57} + 7 \arctan \frac{1}{239} - 12 \arctan \frac{1}{682} + 24 \arctan \frac{1}{12943},
\]

and

\[
\frac{\pi}{4} = 12 \arctan \frac{1}{49} + 32 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239} + 12 \arctan \frac{1}{110443}.
\]
How to verify such identities with a computer?

\[
\arctan x + \arctan y = \arctan \frac{x + y}{1 - xy}
\]

Let us check Machin’s formula

\[
\frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239}.
\]

sage: combine(x,y) = (x+y)/(1-x*y)
sage: combine(1/5,1/5)
5/12

Thus

\[
2 \arctan \frac{1}{5} = \arctan \frac{5}{12}
\]
sage: combine(5/12, 5/12)
120/119

Thus

$$4 \arctan \frac{1}{5} = \arctan \frac{120}{119}$$

sage: combine(120/119, -1/239)
1

Thus

$$4 \arctan \frac{1}{5} - \arctan \frac{1}{239} = \arctan 1 = \frac{\pi}{4}$$
We can “multiply” an arc-tangent by a positive integer $n$:

```sage
sage: muln = lambda x,n: x if n==1 else combine(x,muln(x,n-1))
```

Then we get:

```sage
sage: muln(1/5,4)
120/119
```

and:

```sage
sage: combine(muln(1/5,4),-1/239)
1
```
Symbolic transformations

sage: muln(1/x,2).normalize()
2*x/(x^2 - 1)

2 \arctan \frac{1}{x} = \arctan \frac{2x}{x^2 - 1}

sage: muln(1/x,3).normalize()
(3*x^2 - 1)/((x^2 - 3)*x)

3 \arctan \frac{1}{x} = \arctan \frac{3x^2 - 1}{x^3 - 3x}

sage: muln(1/x,4).normalize()
4*(x^2 - 1)*x/(x^4 - 6*x^2 + 1)

4 \arctan \frac{1}{x} = \arctan \frac{4x(x^2 - 1)}{x^4 - 6x^2 + 1}

What if Gauss had had a computer?
How to discover such identities?

- experimentally with Pari/GP `lindep`
- with Gaussian integers
- a direct method using integers only

What if Gauss had had a computer?
On page 481, Gauss writes for \( p = 5, 13, \ldots \) which \( a^2 + 1 \) have \( p \) as largest prime factor:

\begin{align*}
5 & \mid 2, 3, 7 \\ 13 & \mid 5, 8, 18, 57, 239
\end{align*}

We can (re)discover some identities using Pari/GP as follows:

\begin{verbatim}
? lindep([atan(1/2),atan(1/3),Pi/4])
%7 = [-1, -1, 1]~
? lindep([atan(1/5),atan(1/8),atan(1/18),Pi/4])
%9 = [-3, -2, 1, 1]~
? lindep([atan(1/8),atan(1/18),atan(1/57),Pi/4])
%11 = [-5, -2, -3, 1]~
? lindep([atan(1/18),atan(1/57),atan(1/239),Pi/4])
%13 = [-12, -8, 5, 1]~
\end{verbatim}

What if Gauss had had a computer?
Take all numbers $a$ such that $a^2 + 1$ has all its factors $\leq 13$:

? lindep([atan(1/2), atan(1/3), atan(1/5), atan(1/7), atan(1/8),
           atan(1/18), atan(1/57), atan(1/239), Pi/4])
%1 = [-1, 1, 0, 1, 0, 0, 0, 0, 0]~

Thus $\arctan(1/2) = \arctan(1/3) + \arctan(1/7)$:

sage: combine(1/3, 1/7)
1/2

We can thus omit $\arctan(1/2)$.

? lindep([atan(1/3), atan(1/5), atan(1/7), atan(1/8), atan(1/18),
           atan(1/57), atan(1/239), Pi/4])
%2 = [-1, 1, 0, 1, 0, 0, 0, 0, 0]~

Thus $\arctan(1/3) = \arctan(1/5) + \arctan(1/8)$:

sage: combine(1/5, 1/8)
1/3

We can thus omit $\arctan(1/3)$.
\[ \text{lindep([atan(1/5), atan(1/7), atan(1/8), atan(1/18), atan(1/57),}
\text{ atan(1/239), Pi/4])} \]

\[ \%3 = [-1, 1, 0, 1, 0, 0, 0] \]

Thus \( \arctan(1/5) = \arctan(1/7) + \arctan(1/18) \).

\[ \text{lindep([atan(1/7), atan(1/8), atan(1/18), atan(1/57), atan(1/239), Pi/4])} \]

\[ \%4 = [-1, 1, 0, 1, 0, 0, 0] \]

Thus \( \arctan(1/7) = \arctan(1/8) + \arctan(1/57) \).

\[ \text{lindep([atan(1/8), atan(1/18), atan(1/57), atan(1/239), Pi/4])} \]

\[ \%5 = [1, -2, -1, 1, 0, 0] \]

\[ \arctan(1/8) = 2 \arctan(1/18) + \arctan(1/57) - \arctan(1/239) \]

\[ \text{lindep([atan(1/18), atan(1/57), atan(1/239), Pi/4])} \]

\[ \%6 = [-12, -8, 5, 1] \]

We find Gauss’ 1st formula:

\[ \frac{\pi}{4} = 12 \arctan \frac{1}{18} + 8 \arctan \frac{1}{57} - 5 \arctan \frac{1}{239} \]

What if Gauss had had a computer?
Reducible and irreducible arctangent

We say that \( \arctan(1/n) \) is **reducible** if it can be expressed as a linear combination of smaller arctangents. Otherwise it is **irreducible**.

For \( 1 \leq n \leq 20 \), we have 6 reducible arctangents:

\[
\begin{align*}
\end{align*}
\]
Which primes $p$ can divide $a^2 + 1$?

$p$ divides $a^2 + 1$ is equivalent to $a^2 \equiv -1 \mod p$

Thus $-1$ should be a quadratic residue modulo $p$.

In other words the Jacobi symbol $\left(\frac{-1}{p}\right)$ should be 1.

sage: [p for p in prime_range(3,110) if (-1).jacobi(p) == 1]
[5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109]

We find the primes appearing on the bottom of page 481.

By the first supplement to quadratic reciprocity, only 2 and primes of the form $4k + 1$ can appear.
How to find the $a^2 + 1$ with largest factor $p$?

sage: def largest_prime(n):
....:     l = factor(n)
....:     return l[len(l)-1][0]
sage: largest_prime(1001)
13

sage: def search(p,B):
....:     for a in range(1,B):
....:         if largest_prime(a^2+1)==p:
....:             print a
sage: search(5,10^6)
2
3
7

What if Gauss had had a computer?
Faster way of searching: if $p$ divides $a^2 + 1$, then $r := a \mod p$ is one of the roots of $x^2 + 1 \mod p$:

sage: def search2(p,B):
....:     r = (x^2+1).roots(ring=GF(p))
....:     for t, _ in r:
....:         for a in range(ZZ(t), B, p):
....:             if largest_prime(a^2+1) == p:
....:                 print a

sage: search2(5, 10^6)
3
2
7

We check only 2 values out of $p$. 
Gaussian Integers

Gaussian integers are of the form $a + ib$, with $a, b \in \mathbb{Z}$.

They form an unique factorization domain, with units $\pm 1, \pm i$.

$$17 + i = -i(1 + i)(2 + i)(5 + 2i)$$

```
sage: ZZI.<I> = GaussianIntegers()
sage: factor(17+I)
(I) * (-I - 2) * (I + 1) * (2*I + 5)
```

A Gaussian integer like $5 + 2i$ that cannot be factored is called irreducible.
The Gaussian Integers Method

A term \( \arctan \frac{b}{a} \) corresponds to the Gaussian integer \( a + ib \).

A term \( k \arctan \frac{b}{a} \) corresponds to \( (a + ib)^k \).

A sum \( \arctan \frac{b}{a} + \arctan \frac{d}{c} \) corresponds to \( (a + ib)(c + id) \).

We thus want to find a product of Gaussian integers whose argument is a (non-zero) multiple of \( \pi/4 \).
Example:
\[ \arctan\left(\frac{1}{2}\right) + \arctan\left(\frac{1}{3}\right) = \arctan(1) \]
Machin’s formula in terms of Gaussian integers

\[
\text{sage: } ZZI.<I> = GaussianIntegers() \\
\text{sage: } \text{factor}((5+I)^4) \\
(-3*I - 2)^4 * (I + 1)^4 \\
\text{sage: } \text{factor}(239+I) \\
(I) * (-3*I - 2)^4 * (I + 1)
\]

Thus \(4 \arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right)\) corresponds to \(-i(1 + i)^3\), i.e., to \(9\pi/4\), i.e., \(\pi/4\) modulo \(2\pi\).

\[
\text{sage: } (5+I)^4*(239-I) \\
114244*I + 114244
\]

What if Gauss had had a computer?
Norm of Gaussian Integers

Definition: The norm of $a + ib$ is $N(a + ib) := a^2 + b^2$.

The norm is **multiplicative**: if $a + ib = (b + id)(e + if)$, then $N(a + ib) = N(b + id)N(e + if)$.

\[
(b + id)(e + if) = (be - df) + i(bf + de)
\]

\[
N((b + id)(e + if)) = (be - df)^2 + (bf + de)^2
= (be)^2 + (df)^2 + (bf)^2 + (de)^2
= (b^2 + d^2)(e^2 + f^2)
\]
The Gaussian Integers Algorithm

The term arctan(1/a) corresponds to Gaussian integers a + i, thus to the norm a^2 + 1.

If a^2 + 1 has only few small prime divisors, then a + i can have only few irreducible factors, since their norm must divide a^2 + 1.

Algorithm:

- Input: a set S of primes, a bound A
- factor a^2 + 1 for a up to some bound A;
- identify those a^2 + 1 with only prime divisors in S;
- factor the corresponding Gaussian integers a + i;
- find linear combinations to cancel the exponents of irreducible factors other that 1 + i (up to an unit).

With S = \{2, 5, 13, 17\}, there are 15 values of a up to A = 10^6:

1, 2, 3, 4, 5, 7, 8, 13, 18, 21, 38, 47, 57, 239, 268
This is related to the roots of $x^2 + 1$ modulo 2, 5, 13, 17:

sage: for p in [2, 5, 13, 17]:
    ....:     print p, (x^2+1).roots(ring=GF(p))
2 [(1, 2)]
5 [(3, 1), (2, 1)]
13 [(8, 1), (5, 1)]
17 [(13, 1), (4, 1)]

$a = 268$ corresponds to the roots 3 mod 5, 8 mod 13, 13 mod 17:

sage: crt([3, 8, 13], [5, 13, 17])
268
sage: factor(268^2+1)
5^2 * 13^2 * 17

If we take the other root 4 modulo 17, we get $a = 463$, but $a^2 + 1$ has a spurious prime factor 97:

sage: crt([3, 8, 4], [5, 13, 17])
463
sage: factor(463^2+1)
2 * 5 * 13 * 17 * 97

What if Gauss had had a computer? 37/43
Todd’s reduction process

Idea: decompose $N + i$ into a product $(l_1 \pm i)(l_2 \pm i) \cdots (l_k \pm i)$.

Example for $N = 580$:

```sage
sage: factor(580^2+1)
13 * 113 * 229
```

The least integer $m$ such that $p = 229$ divides $m^2 + 1$ is $m = l_1 = 107$.

If $N + l_1$ is divisible by $p$, then we take $l_1 - i$, else we take $l_1 + i$.

We compute the next residue by multiplying by the conjugate and dividing by $p$:

```sage
sage: (580+I)*(107+I)/229
3*I + 271
```
Todd’s reduction process (continued)

We continue the reduction from $271 + 3i$:

```sage
defactor(271^2+3^2)
2 * 5^2 * 13 * 113
```

The least integer such that $p = 113$ divides $m^2 + 1$ is $m = 15$. Since $271 + 3 \cdot 15$ is not divisible by 113, we take $15 + i$:

```sage
(271+3*I)*(15-I)/113/2
-I + 18
```

At the end of Todd’s reduction process we get:

$$\arctan \frac{1}{580} = - \arctan 1 + 2 \arctan \frac{1}{2} - \arctan \frac{1}{5} + \arctan \frac{1}{15} - \arctan \frac{1}{107}$$
Other identities

\[
\arctan \frac{1}{n} = \arctan \frac{1}{n + 1} + \arctan \frac{1}{n^2 + n + 1}
\]

\[
\arctan \frac{1}{n} = 2 \arctan \frac{1}{2n} - \arctan \frac{1}{4n^3 + 3n}
\]

If we use the latter in Machin’s formula, we can replace \( \arctan(1/5) \) by \( 2 \arctan(1/10) - \arctan(1/515) \), which gives:

\[
\frac{\pi}{4} = 8 \arctan \frac{1}{10} - \arctan \frac{1}{239} - 4 \arctan \frac{1}{515}
\]

discovered by the Scottish mathematician Robert Simson in 1723.
Gauss’ work can be reproduced using modern computational tools.

We can provide algorithms to check or discover identities.

Using computers, we can find identities with large denominators.

But some open questions still remain...
References

https://gallica.bnf.fr/ark:/12148/bpt6k99402s/f483: Gauss’ factorization tables of $a^2 + 1, \ldots, a^2 + 4, a^2 + 81$


Calculation of $\pi$ to 100,000 Decimals, Daniel Shanks and John W. Wrench, Jr., Mathematics of Computation, 1962.


What if Gauss had had a computer?
Solution complète en nombres entiers de l’équation
\[ m \arctan(1/x) + n \arctan(1/y) = k\pi/4, \]
Carl Störmer, Bulletin de la SMF, 1899.

https://en.wikipedia.org/wiki/Machin-like_formula#

Derivation: Machin-like formula on Wikipedia

http://www.machination.eclipse.co.uk/: a database of Machin-like identities, by Hwang Chien-lih and Michael R. Wetherfield