On Numbers of the Form \(n^4 + 1\)

By Daniel Shanks

1. The Number of Primes. Let \(Q_1(N)\) be the number of primes of the form \(n^4 + 1\) for \(1 \leq n \leq N\). By a double sieve argument similar to that used for primes of the form \(n^2 + a\), [1], and for Gaussian twin primes, [2], one is led to the following conjecture:

\[
Q_1(N) \sim \frac{1}{4} s_1 \int_2^N \frac{dn}{\log n}
\]

where

\[
s_1 = \prod_{p \equiv 1 \pmod{4}} \left[ 1 - \frac{\left( \frac{-1}{p} \right) + \frac{2}{p} + \frac{-2}{p}}{p - 1} \right],
\]

the product being taken over all odd primes with \(\left( \frac{a}{p} \right)\) the Legendre symbol. Now

\[
\frac{s_1 L_1(1) L_2(1) L_{-4}(1)}{\zeta^4(2)} = \prod_{p \equiv 8m + 1} \left( 1 - \frac{4}{p} \right) \left( \frac{p + 1}{p - 1} \right)^2
\]

where this product is taken over all primes of the form \(8m + 1\) and \(L_a(s)\) and \(\zeta_a(s)\) are as defined in [1, p. 323]. We may therefore write

\[
s_1 = \frac{\pi^2}{4 \log (1 + \sqrt{2})} \prod_{p \equiv 8m + 1} \left( 1 - \frac{4}{p} \right) \left( \frac{p + 1}{p - 1} \right)^2.
\]

To evaluate this slowly convergent product we use the identity

\[
1 - 4x = \left( \frac{1 - x}{1 + x} \right)^2 \left( \frac{1 - x^2}{1 + x^2} \right)^4 \left( \frac{1 - x^4}{1 + x^4} \right)^8 \left( \frac{1 - x^8}{1 + x^8} \right)^{16} \cdots,
\]

which is valid for \(x < \frac{1}{2}\), and the identity

\[
\frac{\zeta^2(2s)}{\zeta(s) L_1(s) L_2(s) L_{-4}(s)} = \prod_{p \equiv 8m + 1} \left( \frac{p^s - 1}{p^s + 1} \right)^2,
\]

which is valid for \(s > 1\). From tables of \(\zeta_a(s)\) and \(L_a(s)\) we thus obtain

\[
s_1 = 2.67896 \cdots
\]

and therefore

\[
Q_1(N) \sim Q_1(N) = 0.66974 \int_2^N \frac{dn}{\log n}.
\]

It is interesting to compare this formula with that for the conjectured number [1] of primes of the form \(n^2 + 1\),

\[
P_1(N) \sim P_1(N) = 0.68641 \int_2^N \frac{dn}{\log n}.
\]

Received November 1, 1960.
ON NUMBERS OF THE FORM $n^4 + 1$

Table 1

<table>
<thead>
<tr>
<th>$N$</th>
<th>$Q_i(N)$</th>
<th>$\hat{Q}_i(N)$</th>
<th>$Q_i/\hat{Q}_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>18</td>
<td>19.5</td>
<td>0.924</td>
</tr>
<tr>
<td>200</td>
<td>30</td>
<td>32.9</td>
<td>0.911</td>
</tr>
<tr>
<td>300</td>
<td>44</td>
<td>45.1</td>
<td>0.976</td>
</tr>
<tr>
<td>400</td>
<td>52</td>
<td>56.5</td>
<td>0.920</td>
</tr>
<tr>
<td>500</td>
<td>63</td>
<td>67.5</td>
<td>0.934</td>
</tr>
<tr>
<td>600</td>
<td>75</td>
<td>78.1</td>
<td>0.960</td>
</tr>
<tr>
<td>700</td>
<td>80</td>
<td>88.4</td>
<td>0.905</td>
</tr>
<tr>
<td>800</td>
<td>94</td>
<td>98.6</td>
<td>0.934</td>
</tr>
<tr>
<td>900</td>
<td>98</td>
<td>108.5</td>
<td>0.903</td>
</tr>
<tr>
<td>1000</td>
<td>109</td>
<td>118.3</td>
<td>0.922</td>
</tr>
</tbody>
</table>

The coefficients are nearly equal and have analogous formulae:

$$0.68641 = \frac{1}{2} \prod_{p \equiv 1}^{\infty} \left[ 1 - \frac{(-1)^{p-1}}{p-1} \right]$$

$$0.66974 = \frac{1}{4} \prod_{p \equiv 1}^{\infty} \left[ 1 - \frac{(-1)^{p-1} + \frac{2}{p} + \frac{-2}{p}}{p-1} \right].$$

2. A Table. A comparison of $\hat{Q}_i(N)$ with the actual counts $Q_i(N)$ is handicapped by the very rapid increase in $n^4 + 1$. The 109th prime is already $984,095,744,257$, nearly a trillion. A. Gloden [3] has completed the factorization of all $n^4 + 1$ up to $n = 1000$, following the work of Cunningham and others. He has kindly counted the primes for us, where $400 < n \leq 1000$, and using his results we present Table 1. The deviations of $Q_i/\hat{Q}_i$ from unity are not unduly large considering the relatively small upper limit for $N$. For $P_i(N)$ and for the ordinary prime count $\pi(N)$ we have similar deviations for $N = 1000$; $\pi(1000)/\hat{\pi}(1000) = 0.951$ and $P_i(1000)/\hat{P}_i(1000) = 0.924$.

3. Four Classes of Numbers. When we consider that Euler determined $P_i(N)$ up to $N = 1500$ over two hundred years ago [4], the present table of $Q_i(N)$ up to $N = 1000$ seems rather meager. The much greater difficulty of factoring the $n^4 + 1$ numbers is fundamentally due to their much greater magnitude—but there are interesting technical differences also. The sieve method for $n^4 + 1$ used by Gloden, Cunningham, and others has three phases.

A. Compile a list of primes of the form $8m + 1$
B. For each such prime solve the congruence

$$\begin{cases} x^4 \equiv -1 \pmod{p} \\ x < p \end{cases}$$

for its four roots. (Given one solution $x_1$, the remaining three are congruent to $-x_1$, $x_1^3$, and $-x_1^3$.)

C. With each $x$ and each $p$ divide out a factor of $p$ for each $n = x_i + mp$. Similarly determine those $n^4 + 1$ divisible by $p^2$, $p^3$, etc.
Now unfortunately there is much waste computation here. For instance, the hundred \( n^4 + 1 \) for \( n \leq 100 \) have 122 different primes of the form \( 8m + 1 \) as factors. Yet all 295 of the \( 8m + 1 \) primes \( < 100^2 \) must be examined in phases A and B, since \textit{a priori} any such prime may be a factor of the \( n^4 + 1 \). And clearly this waste increases rapidly with \( N \)—for \( N = 1000 \) we must examine all 19552 of the \( 8m + 1 \) primes \( < 1000^2 \) to factor out the (approximately) 1300 distinct actual prime factors.

On the contrary, in the author's sieve \[5\] for \( n^2 + 1 \) there is no waste computation and no phases A and B, either. The primes arise automatically in the sieve itself, together with the corresponding solutions of the congruence, \( x^2 = -1 \pmod{p} \).

This significant difference comes about as follows. For every \( n, n^2 + 1 \) either has no new prime factor (\( n \) is "reducible") or it has precisely one new prime factor—and that to the first power (\( n \) is "irreducible"). Therefore, if all prime factors corresponding to smaller values of \( n \) have already been sieved out, each new prime stands exposed at the smallest \( n \) which satisfies \( n^2 = -1 \pmod{p} \). But for \( n^4 + 1 \) we have not two but \textit{four} classes of \( n \); there are either 0, 1, 2, or 3 new prime factors in \( n^4 + 1 \). It is the occurrence of the "double" and "triple" irreducibles (i.e., 2 and 3 new primes) which prevents the use of the automatic, \( n^2 + 1 \) type sieve for \( n^4 + 1 \). Already for \( n = 10 \) we have a double irreducible

\[ 10^4 + 1 = 73 \cdot 137, \]

with the two new primes 73 and 137.

Let \( R(N), I_1(N), I_2(N) \) and \( I_3(N) \) be the number of "reducibles" (no new prime) and single, double, and triple irreducibles respectively which are \( \leq N \). For example, \( I_1(120) = 92 \) and \( I_2(120) = 28 \). Further, \( R(120) = I_1(120) = 0 \), since neither reducibles nor triple irreducibles arise for \( n \leq 120 \). For larger \( n \) (from Golen's tables) we find both reducibles

\[ 29588^4 + 1 = 17^2 \cdot 41 \cdot 113 \cdot 1249 \cdot 16073 \cdot 28513 \]

and triple irreducibles

\[ 23762^4 + 1 = 637489 \cdot 693569 \cdot 721057, \]

but they are rare.

The mean number of new primes is

\[ \nu(N) = \frac{I_1(N) + 2I_2(N) + 3I_3(N)}{N}, \]

and in analogy with the situation for \( n^2 + 1 \) the question arises whether \( \nu(N) \) has a limit for \( N \rightarrow \infty \). For \( n^2 + 1 \), John Todd [5, p. 83] has conjectured \( \nu(N) \rightarrow \log 2 = 0.693 \). For \( n^4 + 1 \) and a modest \( N \) we have \( \nu(N) \approx 1.3 \). Analogy with Todd's results concerning \( n^2 + 1 \) and \( \log 2 \) would suggest a limit of \( \log 4 \) for \( n^4 + 1 \), but there is no serious evidence in favor of this.

Applied Mathematics Laboratory
David Taylor Model Basin
Washington 7, District of Columbia

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use


4. L. E. Dickson, History of the Theory of Numbers, Stechert, New York, 1934, v. 1, p. 381. According to Dickson, Euler (1752) gave \( P(1500) = 161 \), which is correct, and \( Q(34) = 8 \), which is incorrect—he omits the prime \( 28^2 + 1 \).