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 $1 \leqq n \leqq N$. 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:

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

where

$$s_1 = \prod_{p=3}^{\infty} \left[1 - \frac{\left(\frac{-1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{-2}{p}\right)}{p - 1} \right], \tag{2}$$

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

$$\frac{s_1 L_{-1}(1) L_2(1) L_{-2}(1)}{\zeta_1^2(2)} = \prod_{p=8m+1} \left(1 - \frac{4}{p}\right) \left(\frac{p+1}{p-1}\right)^2 \tag{3}$$

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

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

To evaluate this slowly convergent product we use the identity

$$1 - 4x = \left(\frac{1-x}{1+x}\right)^2 \left(\frac{1-x^2}{1+x^2}\right)^4 \left(\frac{1-x^3}{1+x^3}\right)^{10} \left(\frac{1-x^4}{1+x^4}\right)^{32} \cdots, \tag{5}$$

which is valid for $x < \frac{1}{4}$, and the identity

$$\frac{\zeta_1^2(2s)}{\zeta_1(s) L_1(s) L_2(s) L_{-2}(s)} = \prod_{p=8m+1} \left(\frac{p^s - 1}{p^s + 1}\right)^2, \tag{6}$$

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

$$s_1 = 2.67896 \cdots \tag{7}$$

and therefore

$$Q_1(N) \sim \bar{Q}_1(N) = 0.66974 \int_2^N \frac{dn}{\log n}. \tag{8}$$

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

$$P_1(N) \sim \bar{P}_1(N) = 0.68641 \int_2^N \frac{dn}{\log n}. \tag{9}$$

Received November 1, 1960.

TABLE 1

N	$Q_1(N)$	$\bar{Q}_1(N)$	$Q_1/\bar{Q}_1$
100	18	19.5	0.924
200	30	32.9	0.911
300	44	45.1	0.976
400	52	56.5	0.920
500	63	67.5	0.934
600	75	78.1	0.960
700	80	88.4	0.905
800	94	98.6	0.954
900	98	108.5	0.903
1000	109	118.3	0.922

The coefficients are nearly equal and have analogous formulae:

$$
\begin{aligned}
0.68641 &= \frac{1}{2}\prod_{p=3}^{\infty}\left[1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right] \\
0.66974 &= \frac{1}{4}\prod_{p=3}^{\infty}\left[1 - \frac{\left(\frac{-1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{-2}{p}\right)}{p-1}\right].
\end{aligned} \tag{10}
$$

2. A Table. A comparison of $\bar{Q}_1(N)$ with the actual counts $Q_1(N)$ 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 $400 < n \leqq 1000$, and using his results we present Table 1. The deviations of $Q_1/\bar{Q}_1$ from unity are not unduly large considering the relatively small upper limit for N. For $P_1(N)$ and for the ordinary prime count $\pi(N)$ we have similar deviations for $N = 1000$; $\pi(1000)/li(1000) = 0.951$ and $P_1(1000)/\bar{P}_1(1000) = 0.924$.

3. Four Classes of Numbers. When we consider that Euler determined $P_1(N)$ up to $N = 1500$ over two hundred years ago [4], the present table of $Q_1(N)$ 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 $n \leqq 100$ 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 *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, $x^2 \equiv -1 \pmod p$.

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 $n^2 \equiv -1 \pmod p$. But for $n^4 + 1$ we have not two but *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 $\leqq N$. For example, $I_1(120) = 92$ and $I_2(120) = 28$. Further, $R(120) = I_3(120) = 0$, since neither reducibles nor triple irreducibles arise for $n \leqq 120$. For larger n (from Gloden'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

$$\nu(N) = \frac{I_1(N) + 2I_2(N) + 3I_3(N)}{N}, \tag{11}$$

and in analogy with the situation for $n^2 + 1$ the question arises whether $\nu(N)$ has a limit for $N \to \infty$. For $n^2 + 1$, John Todd [5, p. 83] has conjectured $\nu(N) \to \log 2 = 0.693$. 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

1. Daniel Shanks, "On the conjecture of Hardy and Littlewood concerning the number of primes of the form $n^2 + a$," *Math. Comp.*, v. 14, 1960, p. 321–332.

2. Daniel Shanks, "A note on Gaussian twin primes," *Math. Comp.*, v. 14, 1960, p. 201–203.

3. A. Gloden, "A note on factors of $n^4 + 1$," *Math. Comp.*, v. 14, 1960, p. 278–279. Also see RMT 42, *Math. Comp.*, v. 14, 1960, p. 284. For earlier bibliography see RMT 109, *MTAC*, v. 11, 1957, p. 274, and RMT 2, *MTAC*, v. 12, 1958, p. 63.

4. L. E. Dickson, *History of the Theory of Numbers*, Stechert, New York, 1934, v. 1, p. 381. According to Dickson, Euler (1752) gave $P_1(1500) = 161$, which is correct, and $Q_1(34) = 8$, which is incorrect—he omits the prime $28^4 + 1$.

5. Daniel Shanks, "A sieve method of factoring numbers of the form $n^2 + 1$," *MTAC*, v. 13, 1959, p. 78–86.