Some Remarks and Problems in Number Theory Related to the Work of Euler

PAUL ERDŐS
Hungarian Academy of Science
Budapest, Hungary

UNDERWOOD DUDLEY
DePauw University
Greencastle, IN 46135

Motto. *One is mathematics and Euler is its prophet.* This phrase was coined half as a joke at a mathematical party in Budapest about 50 years ago by Tibor Gallai. In these remarks we mention some of the things the prophet Euler has handed down to us and sometimes give some later developments. Many of the recollections and conjectures in these remarks are those of the first author, and first person references are used to keep the exposition informal.

In 1737 Euler proved that the number of primes was infinite by showing that the sum of their reciprocals diverges, i.e.,

$$\sum_{p \text{ prime}} \frac{1}{p} = \infty. \tag{1}$$

He did this by using the (invalid) identity

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} \left(1 - \frac{1}{p}\right)^{-1}$$

Though invalid—Euler rarely worried about convergence—it can be fixed by looking at

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}$$

as $s \to 1$. For this, see Ayoub [1], who said elsewhere [2] that Euler "laid the foundations of analytic number theory."

Denote by $\pi(x)$ the number of primes $p \leqslant x$. It is curious that Euler after having proved (1) never asked himself: how does $\pi(x)$ behave for large x? For (1) immediately implies that for infinitely many x, $\pi(x) > x^{1-\epsilon}$. In fact, for infinitely many x, $\pi(x) > x/(\log x)^{1+\epsilon}$. It seems to me that with a little experimentation Euler could have discovered the prime number theorem

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

After all, he did discover the quadratic reciprocity theorem by observation, and that seems to be at least as hard to see. But as we will see again later, such questions did not seem to occur to Euler. The prime number theorem was first conjectured shortly before Euler's death by Legendre in 1780 in the form

$$\pi(x) \approx \frac{x}{\log x - c},$$

with $c \approx 1.08$. In 1792 Gauss, who was only 15 at the time, even noticed that

$$\int_2^x \frac{dy}{\log y} = \sum_{k=2}^{x} \frac{1}{\log k} + O(1)$$

gives a much better approximation to $\pi(x)$ than $x/\log x$, a most remarkable achievement! Again, it is strange that Gauss and others did not prove that

$$\frac{c_1 x}{\log x} < \pi(x) < \frac{c_2 x}{\log x}$$

and that if $\lim_{x\to\infty} \pi(x)/(x/\log x)$ exists, then it must be 1. All these results were proved by Tchebychef around 1850. Both Euler and Gauss could easily have proved all this. The prime number theorem was first proved by Hadamard and de la Vallée Poussin in 1896 using analytic functions, which were not available to Euler and Gauss.

More than 40 years ago, I conjectured that if $1 \leqslant a_1 < a_2 < \cdots$ is a sequence of integers for which

$$\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty, \tag{2}$$

then the sequence $\{a_n\}$ contains arbitrarily long arithmetic progressions. This conjecture is still not settled; I offer \$3,000 for its proof or disproof. If my conjecture is true, then Euler's result that $\Sigma 1/p$ diverges immediately implies that the primes contain arbitrarily long arithmetic progressions. Until this year, the longest such progression known was due to Weintraub [33] and has 17 terms: $3430751869 + 87297210t$, $t = 0, 1, \ldots, 16$. With patience and a good computer one could probably find more primes in arithmetic progression. In fact, 18 such primes were found by P. Pritchard, who reported this in January 1983 at the AMS meeting in Denver. The discovery was also described in *The Chronicle of Higher Education*, 2/9/83, p. 27.

It often happens that a problem on primes can be solved by generalizing it, and proving it for some more general sequences which share some property with the primes, such as being equally numerous. Even using this idea, my \$3,000 problem really seems to be very deep. Schur conjectured, and van der Waerden proved [30], that if we divide the integers into two classes, then at least one of the classes contains arbitrarily long arithmetic progressions. Fifty years ago, Turan and I conjectured [13] that if $r_k(n)$ is the smallest integer such that every sequence of integers of the form

$$1 \leqslant a_1 < a_2 < \cdots < a_{r_k(n)} \leqslant n$$

contains an arithmetic progression of k terms, then for every k,

$$\lim_{n\to\infty} \frac{r_k(n)}{n} = 0.$$

This conjecture is clearly stronger than van der Waerden's theorem, but weaker than (2). About 30 years ago K. F. Roth [28] proved the conjecture for $k = 3$. The general conjecture was finally proved by Szemeredi in 1972 [29]. For further information see [14].

A much stronger conjecture on primes states that for every k there are k *consecutive* primes which form an arithmetic progression. The longest known has only six terms: $121174811 + 30t$, $t = 0, 1, \ldots, 5$ [19]. This conjecture is undoubtedly true but is completely unattackable by the methods at our disposal.

Denote by $p(n)$ the **number of unrestricted partitions of** n, that is, the number of ways of writing n as a sum of positive integers. For example, $p(5) = 7$ because $1 + 1 + 1 + 1 + 1 = 2 + 1 + 1 + 1 = 2 + 2 + 1 = 3 + 1 + 1 = 3 + 2 = 4 + 1 = 5$. Leibniz asked Bernoulli about $p(n)$ in 1669, but it was not until Euler saw that

$$1 + \sum_{n=1}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} (1 - x^n)^{-1}$$

and ingeniously proved that

$$\prod_{n=1}^{\infty}(1-x^n)=\sum_{n=-\infty}^{\infty}(-1)^n x^{n(3n+1)/2}$$

that any progress was made. Combining the last two equations gives a recursion relation

$$p(n)=p(n-1)+p(n-2)-p(n-5)-p(n-7)+p(n-12)+\cdots$$

that lets values like $p(200)=397299029388$ [15] be calculated. This was the start of generating functions.

As far as I know, Euler never tried to estimate $p(n)$ as a function of n. Hardy-Ramanujan [15] and Uspensky were the first to obtain the asymptotic formula for $p(n)$,

$$p(n)\sim\frac{1}{4\sqrt{3}\,n}e^{\pi\sqrt{2n/3}}. \tag{3}$$

In 1937 Rademacher [26] found a convergent series for $p(n)$ and later I [11] and Newman [24] gave an elementary proof of (3). These estimates are complicated, but the inequality

$$e^{c_1 n^{1/2}}<p(n)<e^{c_2 n^{1/2}}$$

could very easily have been obtained by Euler. These questions which seem so natural to us now must not have occurred to Euler. It could have been that the idea of function was not yet a natural one. Euler was more concerned with representing integers in various forms. He spent 40 years, off and on, trying to prove that every positive integer is a sum of four squares, only to have Legendre give the first proof in 1770. And think of how much time he must have spent on doing things like the following, finding integers x, y, z, w such that

$x \pm y,\ x \pm z,\ y \pm z$ are all squares (see below and right),

Tabelle

Für die Zahlen, welche in der Form $m^4 - n^4$ enthalten sind.

m	nn	mm − nn	mm + nn	$m^4 - n^4$
4	1	3	5	3. 5
9	1	8	10	16. 5
9	4	5	13	5. 13
16	1	15	17	3. 5. 17
16	9	7	25	25. 7
25	1	24	26	16. 3. 13
25	9	16	34	16. 2. 17
49	1	48	50	25. 16. 2. 3
49	16	33	65	3. 5. 11. 13
64	1	63	65	9. 5. 7. 13
81	49	32	130	64. 5. 13
121	4	117	125	25. 9. 5. 13
121	9	112	130	16. 2. 5. 7. 13
121	49	72	170	144. 5. 17
144	25	119	169	169. 7. 17
169	1	168	170	16. 3. 5. 7. 17
169	81	88	250	25. 16. 5. 11
225	64	161	289	289. 7. 23

Euler's *Algebra* (v. 2, chap. 15, §235, p. 351) contains this table of squares m^2, n^2, their difference and sum, and $m^4 - n^4$ (the left column heading has a printer's error).

$xy \pm x$, $xy \pm y$ are all squares,

$x^2 + y^2$, $x^2 + z^2$, $y^2 + z^2$ are all squares,

$x^2 + y^2 + z^2$, $x^2 + y^2 + w^2$, $x^2 + z^2 + w^2$, $y^2 + z^2 + w^2$ are all squares,

$x + y$ is a square, $x^2 + y^2$ is a cube,

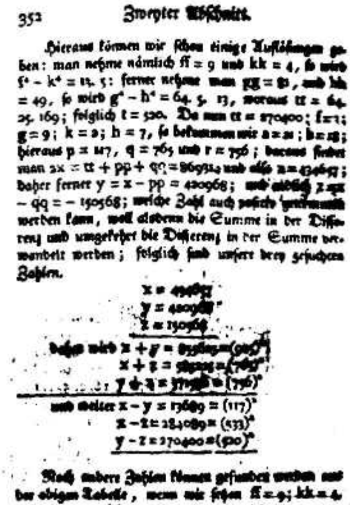
$x + y + z$, $xy + yz + zx$, xyz are all squares,

and so on ([8], ii, XV–XXI). Perhaps not many today are very interested in this.

Euler was the first to consider the function $\phi(n)$, the **number of integers $1 \leqslant m < n$ relatively prime to n**, and this function bears his name (see Glossary). Euler derived a formula equivalent to the well-known

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$$

but he never investigated the function any further, though a great deal of work has been done on it since. It is one more example of Euler's lack of curiosity about functions. There is still a surprising number of unsolved problems about $\phi(n)$. Carmichael conjectured [4] that the number of solutions of $\phi(n) = m$ can never be 1 (i.e., if $\phi(n_1) = m$ then there is an $n_2 \neq n_1$ with $\phi(n_2) = m$). Though the conjecture is known to be true for $m < 10^{400}$ [17], it is probably unattackable by the methods at our disposal. I proved [10] that if there is an integer m for which $\phi(n) = m$ has k solutions, then there are infinitely many integers with this property. If n is prime, $\phi(n) = n - 1$ of course; Lehmer conjectured [21] that $\phi(n)$ divides $(n - 1)$ only if n is prime. This conjecture also seems unattackable. On the other hand, it is an easy exercise to show that $\phi(n)$ divides n if and only if $n = 2^\alpha 3^\beta$. R. L. Graham has conjectured that for every a there are infinitely many n for which $\phi(n)$ divides $n + a$.



352 Zweyter Abschnitt.

Hieraus können wir schon einige Auflösungen geben: man nehme nämlich ff = 9 und kk = 4, so wird f⁴ − k⁴ = 13. 5: ferner nehme man gg = 81, und hh = 49, so wird g⁴ − h⁴ = 64. 5. 13, woraus tt = 64. 25. 169; folglich t = 520. Da nun tt = 270400; f = 3; g = 9; k = 2; h = 7, so bekommen wir [illegible]; hieraus p = 117, q = 765 und r = 756; daraus findet man 2x = tt + pp + qq = 869314 und also x = 434657; daher ferner y = x − pp = 420968; und endlich z = x − qq = − 150568; welche Zahl auch positiv genommen werden kann, weil alsdenn die Summe in der Differenz und umgekehrt die Differenz in der Summe verwandelt werden; folglich sind unsere drey gesuchten Zahlen.

x = 434657
y = 420968
z = 150568

daher wird x + y = 855625 = (925)²
x + z = 585225 = (765)²
y + z = 571536 = (756)²
und weiter x − y = 13689 = (117)²
x − z = 284089 = (533)²
y − z = 270400 = (520)²

Noch andere Zahlen können gefunden werden aus der obigen Tabelle, [illegible]

Euler then demonstrates (p. 352), using his table values, how to obtain integers x, y, z such that sums and differences of any pair of these is a square. In his example, he obtains $x = 434{,}657$, $y = 420{,}968$, $z = 150{,}568$.

The well-known conjecture of Fermat states that $x_1^k + x_2^k = x_3^k$ has no positive integer solutions for $k > 2$. Euler proved the statement for $k = 4$ and almost proved it for $k = 3$ (see [8], ii, XXI, XXII). It has recently been proved by Wagstaff for all $k \leqslant 125{,}000$ [31]. The general conjecture seems to be out of reach at present. Euler conjectured the following generalization:

$$x_k^k = x_1^k + x_2^k + \cdots + x_{k-1}^k$$

has no nontrivial solution in integers for $k \geqslant 3$. This conjecture was disproved by Lander and Parkin [18] who found the equation

$$144^5 = 133^5 + 110^5 + 84^5 + 27^5.$$

This is so far the only known counterexample. The case $k = 4$ seems to be of special interest; in 1948 M. Ward [32] showed that there are no nontrivial solutions for $x_4 \leqslant 10{,}000$, and in 1967 Lander, Parkin and Selfridge [20] extended the result to $x_4 < 220{,}000$. Euler was not even able to find four fourth powers whose sum is a fourth power and it was only in 1911 that the example

$$353^4 = 315^4 + 272^4 + 120^4 + 30^4$$

was found by R. Norrie ([8]; ii, XXII).

In the same direction, Euler gave a complete parametric solution of the equation

$$x^3 + y^3 = u^3 + v^3,$$

namely,

$$x = 1 - (a-3b)(a^2+3b^2) \qquad u = (a+3b) - (a^2+3b^2)^2$$
$$y = (a+3b)(a^2+3b^2) - 1 \qquad v = (a^2+3b^2)^2 - (a-3b)$$

and proved that for infinitely many integers n, $n = x^4 + y^4 = u^4 + v^4$ by giving a complicated parametric solution [16] which includes the smallest solution

$$133^4 + 134^4 = 158^4 + 59^4 = 635{,}318{,}657.$$

After Ramanujan surprised Hardy by knowing that

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

was the smallest integer which is the sum of two cubes in more than one way, Hardy asked him if he knew any integer which was the sum of two fourth powers in more than one way. Ramanujan answered that he did not know any such numbers, and if they existed, they must be very large. Thus, both were unaware of the old work by Euler. It is not yet known if there are any integers which are the sum of two fourth powers in *more* than two ways, i.e., if the number of solutions of $n = x^4 + y^4$ is at most 2.

Denote by $f_3^{(2)}(n)$ the number of solutions of $n = x^3 + y^3$. Mordell proved that $\limsup_{n\to\infty} f_3^{(2)}(n) = \infty$ and Mahler [23] proved that $f_3^{(2)}(n) > (\log n)^{1/4}$ for infinitely many n. As far as I know there is no nontrivial upper bound known for $f_3^{(2)}(n)$. Very likely $f_3^{(2)}(n) < c_1(\log n)^{c_2}$ for all n, if c_1 and c_2 are sufficiently large absolute constants.

Euler was the first to evaluate $\sum_{n=1}^{\infty} 1/n^2$. In 1731 he obtained the sum accurate to 6 decimal places, in 1733 to 20, and in 1734 to infinitely many ($= \pi^2/6$). Ayoub [2] said about his proof that "it opened up the theory of infinite products and partial fraction decomposition of transcendental functions and its importance goes far beyond the immediate application." Euler studied further what we now call the **Riemann ζ-function** ($= \sum_{n=1}^{\infty} n^{-s}$ when $\mathrm{Re}(s) > 1$) and in 1749 he proved the functional equation

$$\zeta(1-s) = \pi^{-s} 2^{1-s} \Gamma(s) \cos\frac{\pi s}{2} \zeta(s)$$

for $s = 1, 2, \ldots$ and said that he was certain it was true for all real s. It was not until 1859 that Riemann proved this.

As far as we know, Euler was the first to define **transcendental numbers** as numbers which are not the roots of algebraic equations. It is perhaps curious that he never proved their existence. The proof of Liouville was well within his reach. Maybe Euler considered the existence of transcendental numbers as self-evident, which by our standards, is certainly not the case.

Of course, not even Euler was perfect. His proofs of Fermat's Last Theorem for exponent 3, as well as his proof that every prime has a primitive root, are considered incomplete by our present standards. He regularly used infinite series without paying any attention to convergence (nevertheless his proofs are almost always correct except for rigor, which is easy to supply).

However, in at least one instance, Euler's intuition completely misled him and he produced a false "proof" which could not be corrected by methods at his disposal. Euler wanted to prove that $\sum_{n=1}^{\infty}\mu(n)/n = 0$, where $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free and $\mu(n) = (-1)^k$ if n is the product of k distinct primes ($\mu(n)$ is known as the Möbius function). He simply argued as follows:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = \prod_{p}(1 - 1/p) = 0. \tag{4}$$

This argument is, of course, inaccurate, since $\sum_{n=1}^{\infty}\mu(n)/n$ is not absolutely convergent and (4) was first proved correctly by von Mangoldt at the end of the nineteenth century. Equation (4) is known to be equivalent to the prime number theorem.

Another error of a different kind was pointed out to me by Mordell. Euler proved that if p divides $x^2 + ny^2$ without dividing both x and y, then p is $u^2 + nv^2$ for $n = 1, 2, 3$. He then used the same arguments for $n = 5$, though Fermat knew long before, and Euler knew too, that the conclusion was not true. (We know now that the reason is that unique factorization fails.) Edwards [9] thinks it was Euler's age, his blindness, or his secretary that may have caused the mistake.

We close with some of the less important things Euler did, to give an idea of his immense range and power. Before Euler, only three pairs of **amicable numbers** were known. These are pairs like 220 and 284, where the sum of the proper divisors of one of the numbers is equal to the other: $110 + 55 + 44 + 22 + 20 + 11 + 10 + 5 + 4 + 2 + 1 = 284$ and $142 + 71 + 4 + 2 + 1 = 220$. The pair (220, 284) was known to Pythagoras; another pair, (17296, 18416), was found by Fermat in 1636; and the pair (9363584, 9437056) was found by Descartes in 1638. In 1750, Euler gave 62 new pairs ([8], i, I). Amicable pairs are still studied. There were 1095 pairs known in 1972 [22] and a 152-digit pair was found in 1974 [27]. In 1955 I showed [12] that if $A(x)$ is the number of amicable pairs (m, n) with $m \leqslant n \leqslant x$, then $\lim_{x\to\infty} A(x)/x = 0$; Pomerance showed in 1981 [25] that $A(x) < xe^{-(\log x)^{1/3}}$. In the other direction, I conjecture that there are infinitely many pairs; in fact, it is likely that $A(x) > cx^{1-\epsilon}$.

In a letter, Goldbach called Euler's attention to **multigrades**: sets of integers with equal sums of different powers, as in

$$1^k + 5^k + 9^k + 17^k + 18^k = 2^k + 3^k + 11^k + 15^k + 19^k$$

for $k = 0, 1, 2, 3, 4$, and Euler proved the first theorems about them. They have been studied a great deal since then. It was also in a letter to Euler that Goldbach made his famous conjecture that every even integer greater than 4 is a sum of two primes, and that has been studied even more than multigrades. There has not been much progress since Chen showed in 1966 [5] that every sufficiently large even integer is a sum of a prime and a product of at most two primes.

Euler discovered that if $p = 4k + 1$ is a prime, then p can be written $p = x^2 + y^2$ in exactly one way; this led him to look for numbers d such that if $n = x^2 + dy^2$ with $(x, y) = 1$ in exactly one way, then n is prime. He found 65 of them, with 1848 the largest ([8], ii, XIV). It seems likely that he found them all, since it is known that their number is finite [6] and there is at most one greater than 10^{65} [7]. So in a way, Euler said the first and last words on this subject.

Euler proved that every **even perfect number** (i.e., equal to the sum of its proper divisors, as $28 = 14 + 7 + 4 + 2 + 1$) is of the form $2^{p-1}(2^p - 1)$ for p and $2^p - 1$ prime and gave the first of a long list of necessary conditions that an odd perfect number will have to satisfy ([8], i, I).

Fermat thought all the Fermat numbers $2^{2^n}+1$ were prime. Euler factored $2^{2^5}+1$ in 1732; $2^{2^7}+1$ was not factored until 1971 [3].

Euler was the first to look at that equation that keeps coming up in popular journals, $x^y = y^x$ ([8], ii, XXIII).

And Euler discovered, no one knows how, that the polynomial $n^2 - n + 41$ is a prime for $n = 1, 2, \ldots, 40$.

If Euler had never done anything *except* number theory, he would still be remembered as one of the great mathematicians.

References

[1] R. Ayoub, Euler and the Zeta function, Amer. Math. Monthly, 81 (1974) 1067–1085.
[2] ______, An Introduction to the Analytic Theory of Numbers, Amer. Math. Soc., Providence, RI, 1963.
[3] J. Brillhart and M. A. Morrison, The factorization of F_7, Bull. Amer. Math. Soc., 77 (1971) 264.
[4] R. D. Carmichael, Note on Euler's ϕ-function, Bull. Amer. Math. Soc., 28 (1922) 109–110.
[5] J. R. Chen, On the representation of a large even integer as the sum of a prime and the product of at most two primes, Kexue Tongbao, 17 (1966) 385–386.
[6] S. Chowla, An Extension of Heilbronn's class-number theorem, Quart. J. Math. Oxford Ser., 5 (1934) 304–307.
[7] S. Chowla and W. E. Briggs, On discriminants of binary quadratic forms with a single class in each genus, Canad. J. Math., 6 (1954) 463–470.
[8] L. E. Dickson, History of the Theory of Numbers, Chelsea, New York, 1952 reprint of the 1919 edition.
[9] H. M. Edwards, The genesis of ideal theory, Arch. Hist. Exact Sci., 23 (1980) 321–378.
[10] P. Erdős, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function, Quart. J. Math. Oxford Ser., 6 (1935) 205–213.
[11] ______, On an elementary proof of some asymptotic formulas in the theory of partitions, Ann. of Math., (2) 43 (1942) 437–450.
[12] ______, On amicable numbers, Publ. Math. Debrecen, 4 (1955) 108–111.
[13] P. Erdős and P. Turan, On some sequences of integers, J. London Math. Soc., 11 (1936) 261–264.
[14] R. L. Graham, B. Rothschild, and J. Spencer, Ramsey Theory, Wiley-Interscience, New York, 1980.
[15] G. H. Hardy and S. Ramanujan, Asymptotic formulae in combinatory analysis, Proc. London Math. Soc., (2) 17 (1918) 75–115.
[16] G. H. Hardy and E. M. Wright, The Theory of Numbers, 4th ed., Oxford U. Press, 1960.
[17] V. J. Klee, Jr., On a conjecture of Carmichael, Bull. Amer. Math. Soc., 53 (1947) 1183–1186.
[18] L. J. Lander and T. R. Parkin, A counterexample to Euler's sum of powers conjecture, Math. Comp., 21 (1967) 101–103.
[19] ______, Consecutive primes in arithmetic progression, Math. Comp., 21 (1967) 489.
[20] L. J. Lander, T. R. Parkin and J. L. Selfridge, A survey of equal sums of like powers, Math. Comp., 21 (1967) 446–453.
[21] D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc., 38 (1932) 745–757.
[22] E. J. Lee and J. S. Madachy, The history and discovery of amicable numbers I, II, III, J. of Recreational Math., 5 (1972) 77–93, 153–173, 231–249.
[23] K. Mahler, On the lattice points of curves of genus 1, Proc. London Math. Soc., (2) 39 (1935) 431–466.
[24] D. J. Newman, The evaluation of the constant in the formula for the number of partitions of n, Amer. J. Math., 73 (1951) 599–601.
[25] C. Pomerance, On the distribution of amicable numbers II, J. Reine Angew. Math., 325 (1981) 183–188.
[26] H. Rademacher, On the partition function $p(n)$, Proc. London Math. Soc., (2) 43 (1937) 241–254.
[27] H. J. J. te Riele, Four large amicable pairs, Math. Comp., 28 (1974) 309–312.
[28] K. F. Roth, On certain sets of integers II, J. London Math. Soc., 29 (1954) 20–26.
[29] E. Szemeredi, On sets of integers containing no k elements in arithmetic progression, Acta Arith., 27 (1975) 199–245.
[30] B. L. van der Waerden, Beweis einer baudetschen Vermuting, Nieuw Arch. Wisk., 15 (1928) 212–216.
[31] S. S. Wagstaff, Jr., The irregular primes to 125,000, Math. Comp., 32 (1978) 583–591.
[32] M. Ward, Euler's problem on fourth powers, Duke Math. J., 15 (1948) 827–837.
[33] S. Weintraub, Seventeen primes in arithmetic progression, Math. Comp., 31 (1977) 1030.