ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 36, Number 4, 2006

ON SOME CONJECTURES RELATED TO THE GOLDBACH CONJECTURE

J. FABRYKOWSKI

ABSTRACT. In the first part of this note we consider the problem of representing integers as a sum of a square and an almost prime and in the second part we turn to investigate distribution of roots of certain class of reciprocal polynomials. In both cases we will show a connection with the celebrated Goldbach conjecture stating that every even integer $2n \geq 4$ can be expressed as a sum of two primes.

1. For a positive integer r let P_r denote a positive integer having at most r prime factors distinct or not. Such an integer P_r is called an almost prime of order r. Obviously, if $r = 1$, then P_1 is a prime number. We consider the problem of representing an integer n in the form $n = m^2 + P_r$, where m is a nonnegative integer. By the definition of P_r it follows that if such representation exists for some r, then it also holds for any $r' > r$, hence one should investigate this problem for a smallest possible r.

If $r = 1$, then it is well known that there are infinitely many integers n which cannot be written in the form m^2+p, for example, no integer of the form $(3k+2)^2$ with $k \geq 1$ is of this form. Therefore we assume $r \geq 2$. Typically, analytic and sieve methods are used to handle problems of this kind and the corresponding results will hold for sufficiently large integers.

The case $r = 3$. Here we make the following observation:

Theorem 1. *Every sufficiently large integer n can be represented in the form*

$$n = m^2 + P_3.$$

Received by the editors on September 24, 2003.

Proof. First we consider the case $n \neq k^2$. The above claim follows from the result on the linear weighted sieve [**5**]:

$$|\{n,\ 1 \leq n \leq x,\ F(n) = P_{g+1}\}| \geq \frac{2}{3} \prod_p \frac{1-\rho(p)/p}{1-1/p} \frac{x}{\log x}, \tag{1}$$

for $x \geq x_0 = x_0(F)$ where $F(n)$ is an irreducible polynomial of degree g (≥ 1) with integer coefficients and $\rho(p)$ is the number of solutions to the congruence $F(a) \equiv 0 \pmod p$ with an additional assumption $\rho(p) < p$ for all p.

This result applies in our case with $F(x) = n - x^2$. It also follows that if n is not a square then there exists a positive constant c such that the number of representations is at least $c(\sqrt{n}/\log n)$.

If $n = k^2$ for some integer k, then our polynomial is reducible and the inequality (1) does not apply. In this case we appeal to the well-known result of Chen [**1**] stating that every sufficiently large even integer $2k$ admits representation in the form:

$$2k = p + P_2. \tag{2}$$

From this it follows that $P_2 - k = k - p$, hence $k - m = p$, and $k + m = P_2$ for some integer m. Multiplying the last two equations we get $n = k^2 = m^2 + pP_2 = m^2 + P_3$ which proves this case.

The case $r = 2$. The above argument underlines a connection between representations of integers as a sum of a square and an almost prime and of even integers written as a sum of two almost primes. The most transparent connection holds in the case $r = 2$ which is expressed as follows:

Theorem 2. *If every integer $n \geq 3$ can be expressed as $n = m^2 + P_2$ in two different ways, then the Goldbach conjecture holds true.*

Proof. Let $n = k^2$, $k \geq 2$, and p, q, r, s be primes, and suppose that k^2 has two different representations in the above form. It is clear that $k^2 = m_1^2 + p = m_2^2 + q$ cannot happen, since each representation implies $k - m_1 = k - m_2 = 1$, hence they are the same representations. If

$k^2 = m_1^2 + p = m_2^2 + sr$, then $k - m_1 = 1$, forcing $k - m_2 = r$ say, and consequently $2k = r + s$. Finally, if $k^2 = m_1^2 + pq = m_2^2 + rs$, then either $k - m_1 = 1$ or $k - m_2 = 1$ but not both. Therefore, either $2k = p + q$ or $2k = r + s$. $\square$

Numerical computation supports the following conjecture:

Conjecture 1. *Every integer $n \geq 3$ can be expressed as $n = m^2 + P_2$ in two different ways.*

This has been verified in the range $1 \leq n \leq 100,000$. If $n \neq k^2$, then we may apply the result of Iwaniec [**2**] which mutatis mutandis can be formulated as follows.

Theorem. *If $G(x) = ax^2 + bx + c$ is an irreducible polynomial with c odd, then*

$$|\{x \leq n;\ G(x) = P_2\}| > C \frac{x}{\log x}$$

for sufficiently large n and positive constant C.

Thus, in our case if n is odd we take $G(x) = n - x^2$, and if n is even, then we take $G(x) = 2l - 1 - 4x - 4x^2$, where $n = 2l$. In both cases the assumption $n \neq k^2$ implies that the polynomials are irreducible.

As we saw above, Conjecture 1 implies the Goldbach conjecture. The assumption that $n = m^2 + P_2$ in two different ways might be replaced by requiring that $m < \sqrt{n} - 1$. If this is the case, then any representation $k^2 = m^2 + P_2$ is equivalent to $2k = p + q$, where $P_2 = pq$ and with $m = (q - p)/2$, $(q \geq p)$. Such a requirement rules out the possibility of $k^2 = m^2 + p$, where p is a prime. In view of this observation, we make another conjecture.

Conjecture 2. *Every integer $n \geq 3$ can be expressed as $n = m^2 + P_2$, where*

$$0 \leq m \leq \sqrt{n} - 1.$$

Again, the Iwaniec result implies that sufficiently large integers $n \neq k^2$ admit such a representation and, as observed above, if $n = k^2$, then the number of such representations is exactly the same as the number of representations of $2k = p + q$ in the Goldbach problem.

Let $E_G(x)$ denote the number of exceptional even integers in the Goldbach conjecture, i.e., $E_G(x) = |\{4 \leq 2n \leq x,\ 2n \neq p+q\}|$, then, as we know (see [**4**]), there exists a positive (effectively computable) constant 2δ such that $E_G(x) < x^{1-2\delta}$. Based on this and the result of Iwaniec we may formulate the following.

Theorem 3. *Let* $E(x) = |\{3 \leq n \leq x,\ n \neq m^2 + P_2,\ 0 \leq m < \sqrt{n} - 1\}|$. *Then there exists a positive* (*effectively computable*) *constant* δ *such that, for all large* x,

$$E(x) < x^{(1/2)-\delta}.$$

We have also investigated the problem of representing integers n in the form $n = m^2 + pq$ where p and q are primes. Let $R(n)$ and $R'(n)$ denote the number of representations of n as above, under the assumptions $0 \leq m$ and $0 \leq m < \sqrt{n} - 1$, respectively. In the range $3 \leq n \leq 100,000$, we found that $R(n) > 0$ and $R'(n) > 0$ for all integers n except $n = 3$, 12, 17, 28, 32, 72, 108, 117, 297 and 657. For large n the expected values of $R(n)$ and $R'(n)$ will attend their local minima at squares, the case of reducible polynomials. On the other hand, we found the following values:

If $n \in [9001,\ 10000]$, then the minimum value of $R(n)$ is 7 and it occurs at $n = 97^2$, and the next smallest value is 8 for $n = 5^2 19^2$, $n = 2^2 2311$ and $n = 2^4 5^4$. In the interval [99001, 100000] the minimum value is 10 for $n = 2^4 79^2$ and the next smallest is 28 for $n = 2^2 67 \cdot 373$ and 42 for $n = 3^4 5^2 7^2$.

It is easy to see that, if $R'(n) > 0$ for $n = k^2$, then $2k = p + q$. We also expect that, for sufficiently large $n \neq k^2$, $R(n) > 0$ and $R'(n) > 0$ might be provable since it is likely that the number of representations of n in the form $m^2 + pq$ exceeds the number of representations in the form $m^2 + p$.

2. In this part we will work with reciprocal polynomials, which are products of the following polynomials of degree four:

$$f_{pq}(x) = (px^2 - 2nx + q)(qx^2 - 2nx + p),$$

where p and q are prime numbers, n is a positive integer and $pq < n^2$.

Let us make several observations. If n is the exceptional Goldbach integer, then obviously 1 is not a root of the polynomial f_{pq}. The polynomial has four real positive roots and, since it is reciprocal, two of them are in the interval $(0, 1)$. Furthermore, it is easy to verify that if $p \neq q$, then all the roots are distinct.

Suppose now that p, q, r, s are pairwise distinct primes, and consider the polynomial:

$$f_{pqrs}(x) = f_{pq}(x) f_{rs}(x).$$

We shall prove the following.

Lemma. *Let p, q and r, s be pairwise distinct odd primes such that $pq < n^2$ and $rs < n^2$. Let α_i, $i = 1, 2, 3, 4$, be the roots of the polynomial f_{pq} and β_j, $j = 1, 2, 3, 4$, the roots of the polynomial f_{rs}. Then $\alpha_k = \beta_l$ implies that $2n = p + q$ and $2n = r + s$.*

Proof. The condition $\alpha_k = \beta_l$ is of the form $[n \pm (\sqrt{n^2 - pq})]/p = [n \pm (\sqrt{n^2 - rs})]/r$ where arbitrary signs $+$ or $-$ can be placed in the numerators. Routine calculation shows that the former equality implies:

$$(rq - ps)^2 = 4n^2(q - s)(r - p). \tag{3}$$

Let us rewrite (3) in the form:

$$[r(q - s) + s(r - p)]^2 = 4n^2(q - s)(r - p), \tag{4}$$

from which it follows that $q > s$ and $r > p$, or $q < s$ and $r < p$. Consider (4) modulo $r - p$. We obtain $r^2(q - s)^2 \equiv 0 \mod (r - p)$. Since $(r, r - p) = 1$, then it follows that $(q - s)^2 \equiv 0 \mod (r - p)$. Similarly, considering (4) modulo $q - s$, we obtain that $(r - p)^2 \equiv 0 \mod (q - s)$. The above two congruences tell us that the even integers $r - p$ and $q - s$ have exactly the same prime divisors. Let t be a prime such that $t^a || q - s$ and $t^b || r - p$, where $a < b$. Then t^{2a} exactly divides the left-hand side of (4), however t^{a+b} divides the right-hand side; hence, we must have $a = b$. It follows that $q - s = r - p = u$, say. Therefore, (4) becomes

$$(r+s)^2u^2 = 4n^2u^2,$$

implying $2n = r + s$. Note that if (4) is changed to the form:

$$[q(r-p) + p(q-s)]^2 = 4n^2(q-s)(r-p),$$

then we would get $2n = p + q$. $\square$

The lemma tells us that if $2n$ is an exceptional Goldbach integer, then for all pairwise distinct primes p, q, r, s, the polynomial f_{pqrs} has all distinct roots, four of them in the interval $(0, 1)$. It can be generalized as follows:

Let P_n be a set of primes such that, for every $p, q \in P_n$, $pq < n^2$, and let T_n be a subset of P_n of even order $2k$, say. Now let $\prod$ be a set of ordered pairs of primes, where all the primes are taken from T_n, and each prime of T_n occurs exactly once in only one ordered pair.

Define

$$f_{\prod} = \prod_{(p,q)\in\prod} f_{pq}.$$

We have the following:

Theorem. *If $2n$ is an exceptional Goldbach integer, then the polynomial $f_{\prod}$ is reciprocal of degree $4k$, it has $4k$ distinct roots such that $2k$ of them are in the interval $(0, 1)$.*

Remark. It also follows from the lemma that if any two roots of the polynomial $f_{\prod}$ are equal, then they must be equal to 1. Moreover, if $2n$ is an exceptional Goldbach integer, then the polynomial $f_{\prod}$ (of degree ≥ 4) has at most four rational roots. It can happen only if $2n = 1 + pq$, where the roots are $1/p, 1/q, p$ and q.

Final comments. Suppose that the polynomial $f_{\prod}$ is of degree $4k$ and that $2n$ is an exceptional Goldbach integer. Then, since $2k$ of its roots are in the interval $(0,1)$, the Dirichlet box principle tells us that two roots exist whose distance is at most $1/2k$. The fact that all the roots are distinct is equivalent to nonvanishing of its discriminant.

There is an interesting result of Mahler [**3**] which relates the minimal distance between the roots of a polynomial and its discriminant.

More precisely, let $m \geq 2$, and $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m = a_0\prod_{i=1}^m (x - \alpha_i)$. Let $P = \prod_{1\leq h<k\leq m}(\alpha_h - \alpha_k)$. Define the discriminant $D(f)$ of the polynomial f by $D(f) = a_0^{2m-2}P^2$. In the case if $\alpha_i \neq \alpha_j$ for $i \neq j$, let $\Delta(f) = \min_{1\leq h<k\leq m}|\alpha_h - \alpha_k|$. Finally, let $M(f) = |a_0|\prod_{h=1}^m \max(1, |\alpha_h|)$ and $L(f) = \sum_{i=1}^m |a_i|$.

Theorem (Mahler). *With the above notations*:

$$\Delta(f) > \sqrt{3}\, m^{-(m+2)/2}|D(f)|^{1/2}M(f)^{-(m-1)} \tag{5}$$

and, moreover, $2^{-m}L(f) \leq M(f) \leq L(f)$.

One may investigate further the zeros of polynomials $f_{\prod}$ using inequality (5). Let us assume that $2n$ is an exceptional Goldbach integer and consider the polynomial f_{pqrs}, where the odd primes p, q, r, s are pairwise distinct.

The determinant of the polynomial f_{pqrs} (in a factored form) is equal to:

$$\begin{aligned} D(f_{pqrs}) = 256&(n^2 - pq)^2(n^2 - rs)^2 \\ &\times (p-q)^4(p+q-2n)^2(p+q+2n)^2 \\ &\times (r-s)^4(r+s-2n)^2(r+s+2n)^2 \\ &\times [(qr-ps)^2 + 4n^2(p-r)(q-s)]^4 \\ &\times [(pr-qs)^2 + 4n^2(p-s)(q-r)]^4. \end{aligned}$$

Since the set P_n has at least $n/\log n$ primes, therefore the set $\prod$ might have at least $n/(2\log n)$ pairs of primes. Hence, there exist two pairs (p,q) and (r,s), say, and two zeros α_{pq} and α_{rs} such that $|\alpha_{pq} - \alpha_{rs}| < (2\log n)/n$. This together with inequality (5) may suggest further investigations of consequences under the assumption that $2n$ is an exceptional Goldbach integer.

REFERENCES

1. J. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica (Sci. China Ser. A) **16** (1973), 157–176.

2. H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. **47** (1978), 171–188.

3. K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. **11** (1964), 257–262.

4. H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1976), 353–370.

5. H.-E. Richert, *Selberg sieve with weights*, Mathematica **16** (1969), 1–22.

Department of Mathematics and Statistics, Youngstown State University, Youngstown, OH 44555
E-mail address: jfabryk@math.ysu.edu