ACTA ARITHMETICA
XCV.2 (2000)

Prime values of reducible polynomials, I

by

YONG-GAO CHEN (Nanjing) and IMRE Z. RUZSA (Budapest)

1. Introduction. It is a generally accepted conjecture that an irreducible integer-valued polynomial without a constant divisor assumes infinitely many prime values at integers. On the other hand, it is easy to see that for a reducible $f \in \mathbb{Q}[x]$ there are only finitely many integers n for which $f(n)$ is prime. It is, however, a nontrivial question to estimate the number of these integers. We shall be primarily interested in finding estimates in terms of the degree of f or of its factors.

In what follows by "polynomial" we always mean a polynomial with rational coefficients, and reducibility is meant in $\mathbb{Q}[x]$. We will write

$$P(f) = \#\{m \in \mathbb{Z} : f(m) \text{ is prime}\}.$$

In this generality probably there is no estimate that depends on the degree alone.

CONJECTURE 1.1. *For every k there is a reducible $f \in \mathbb{Q}[x]$ of degree two such that $P(f) \geq k$.*

To support this conjecture we show that it follows from the following form of the prime k-tuple conjecture: if $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$ are integers such that $a_i \neq 0$ and the polynomial $(a_1x+b_1)\ldots(a_kx+b_k)$ has no constant divisor, then there is an integer y such that all the $a_iy + b_i$ are primes.

Consider now a polynomial

$$f(x) = \frac{x(x+s)}{m},$$

where $m = q_1 \ldots q_k$ is the product of k distinct primes. We want to find an s

---

2000 *Mathematics Subject Classification*: Primary 11N32.

The first author supported by the National Natural Science Foundation of China and Fok Ying Tung Education Foundation. The work was done while he was visiting the Mathematical Institute of the Hungarian Academy of Sciences.

The second author supported by Hungarian National Foundation for Scientific Research, Grants No. T 25617 and T 29759.

such that all the numbers $f(m/q_j)$ are prime. To achieve this we must have $m/q_i + s = q_i p_i$ with primes p_i. This implies that

$$s \equiv -\frac{m}{q_i} \pmod{q_i}$$

for all i, and these congruences together are equivalent to a single congruence $s \equiv S \pmod{m}$. Write $s = S + my$; the numbers that should be prime are

$$\frac{1}{q_i}\left(\frac{m}{q_i} + s\right) = \frac{m}{q_i} y + \frac{1}{q_i}\left(\frac{m}{q_i} + S\right) = a_i y + b_i,$$

say. Observe that $(a_i, b_i) = 1$, since the prime divisors of a_i are the primes q_j, $j \neq i$, and

$$\frac{m}{q_i} + S \equiv S \equiv -\frac{m}{q_j} \not\equiv 0 \pmod{q_j}.$$

We have to exclude the possibility that a prime p always divides at least one of these linear forms. Now if $p \nmid a_i$ then $p \mid a_i y + b_i$ holds for integers y belonging to one residue class modulo p, and if $p \mid a_i$ then it never holds. Thus a sufficient condition is that the number of a_i that are not divisible by p is at most $p-1$. This automatically holds if $p > k$, and it also holds if $p = q_j$ for some j, since in this case $p \mid a_i$ unless $i = j$. These two conditions together cover all primes if $q_1, \ldots, q_k$ are selected so that all primes $\le k$ are included among them. Thus for such choices of the q_j the prime tuple conjecture yields our conjecture above.

The situation changes if we restrict our attention to *integer-valued polynomials*, that is, polynomials such that $f(n)$ is integral whenever so is n.

Theorem 1. *Let*

$$P_n = \sup\{P(f) : \deg f = n,\ f \textit{ is integer-valued and reducible in } \mathbb{Q}[x]\}.$$

We have

$$\exp\left((\log 2 - o(1))\frac{n}{\log n}\right) < P_n < \exp\left(C\frac{n}{\log n}\right)$$

with an absolute constant C.

The second author conjectures that the lower estimate gives the proper order of magnitude. We will establish this under certain restrictions on the degree of the factors of f.

The situation changes considerably if we assume that the factors of f are also integer-valued. Indeed, if $f = gh$ with integer-valued g and h, then $f(x)$ can be a prime only if either $g(x) = \pm 1$ or $h(x) = \pm 1$, which immediately gives $2n$ as an upper bound. The possibility to improve this bound will be the subject of Part II.

2. The upper estimate in Theorem 1. A polynomial of degree n is integer-valued if and only if it has the form

$$f(x) = a_0 + a_1 \binom{x}{1} + \ldots + a_n \binom{x}{n}$$

with integers a_i; thus in particular $n!f(x) \in \mathbb{Z}[x]$. Hence $n!f$ is reducible in $\mathbb{Z}[x]$, say $n!f = gh$. If $f(m)$ is prime, then either $g(m) \mid n!$ or $h(m) \mid n!$. The first possibility yields at most $2\tau(n!)$ possible values for $g(m)$ (where τ denotes the number of positive divisors), hence at most $2\tau(n!) \deg g$ values for m. We have an analogous estimate in the second case, and adding them we obtain

$$P(f) \le 2\tau(n!)(\deg g + \deg h) = 2n\tau(n!). \tag{2.1}$$

To estimate this quantity, observe that for $2 \le k < \sqrt{n}$ and $n/k < p \le n/(k-1)$ we have $p^{k-1} \parallel n!$. From this (by estimating the exponent of primes $\le \sqrt{n}$ crudely by n from above) one easily obtains

$$\tau(n!) = \exp\left((C + o(1))\frac{n}{\log n}\right), \qquad C = \sum_{k=2}^{\infty} \frac{\log k}{k(k-1)}.$$

3. Further upper estimates. In what follows we fix two integers $1 \le d < n$, and try to estimate $P(f)$ for polynomials of degree n which have a divisor h of degree d. Our main result is the following.

THEOREM 2. *Let $1 \le d \le n/2$ be integers, and let f be an integer-valued polynomial of degree n which has a divisor of degree d.*

(i) *We have*

$$P(f) \le 2n^{1+n/d}. \tag{3.1}$$

(ii) *If $d = 1$ or 2, then*

$$P(f) < \exp\left((\log 2 + o(1))\frac{n}{\log n}\right). \tag{3.2}$$

Thus the conjecture after Theorem 1 is confirmed by (ii) for $d = 1, 2$ and by (i) for $d > (\log n)^2/\log 2$.

We say that an integer k is a *constant divisor* of a polynomial g if g is integer-valued and $k \mid g(m)$ for every integer m. We call a polynomial *standard* if it is integer-valued and it has no constant divisor $k > 1$. Clearly any polynomial $g \in \mathbb{Q}[x]$ has a unique representation in the form $g = (b/a)g_1$, where g_1 is standard, a, b are coprime integers and $a \ge 1$.

We start with some preparation and then prove Theorem 2.

LEMMA 3.1. *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree n. The number of integers m for which $|f(m)| \le M$ is at most $2nM^{1/n} + n$.*

Proof. Write

$$f(x) = a(x - x_1)\dots(x - x_n), \qquad x_i \in \mathbb{C}.$$

Here $|a| \ge 1$, thus if $|f(m)| \le M$, then $|m - x_j| \le M^{1/n}$ for at least one j, altogether at most $n(1 + 2M^{1/n})$ possibilities. ■

Lemma 3.2. *Let f be an integer-valued polynomial*, $\deg f \le n$, *and let h be a standard polynomial which divides f. Write $f = (b/a)hg$, where g is standard*, *a, b are coprime integers and $a \ge 1$. Let G and H be the least common denominators of the coefficients of g and h*, *respectively. We have $aGH \mid n!$.*

Proof. Let $h_1 = Hh$ and $g_1 = Gg$; by the definition of G and H, $h_1, g_1 \in \mathbb{Z}[x]$ are primitive polynomials. Since $(a, b) = 1$, b is a constant divisor of f. Hence

$$n!\frac{f}{b} = \frac{n!}{aGH} h_1 g_1 \in \mathbb{Z}[x].$$

Since f_1, g_1 are primitive, so is their product and we see that $aGH \mid n!$. ■

Now consider a fixed standard h and a positive integer n. Take all possible integers a that can occur as a constant divisor of a polynomial gh, where g is a standard polynomial of degree at most $n - d$. By the above lemma we see that always $a \mid n!$. So the collection of these integers a is finite. We define $R(h, n)$ as the l.c.m. of all the possible values of a. The divisibilities $a \mid n!$ imply

$$R(h, n) \mid n!. \tag{3.3}$$

For a prime p, we define α_p as the largest integer α such that there exists a standard polynomial g of degree at most $n - d$ such that p^α is a constant divisor of hg. The above arguments show that always $p^\alpha \mid n!$, thus this maximum is finite and it is 0 for $p > n$. Furthermore we have

$$R(h, n) = \prod_p p^{\alpha_p}.$$

Lemma 3.3. *Let f be an integer-valued polynomial*, $\deg f \le n$, *and let h be a standard polynomial which divides f. Write $f = (b/a)hg$, where g is standard*, *a, b are coprime integers and $a \ge 1$. Let G and H be the least common denominators of the coefficients of g and h*, *respectively. Then for any integer m*, *$(h(m), f(m)) = 1$ implies $h(m) \mid a$, $h(m) \mid n!/H$ and $h(m) \mid R(h, n)$.*

Proof. Since $af(m) = bh(m)g(m)$, the coprimality assumption implies $h(m) \mid a$. Now $a \mid n!/H$ by Lemma 3.2 and $a \mid R(h, n)$ by definition. ■

We define

$$N(h,n)=\max\#\{m\in\mathbb{Z}:(h(m),f(m))=1\},\tag{3.4}$$

where f runs over all integer-valued polynomials of degree n which are multiples of h. This definition is justified by the following lemma. We will see that this somewhat artificial quantity is closely related to $P(f)$.

LEMMA 3.4. *The quantity $N(h,n)$ defined by* (3.4) *is finite and it satisfies*

$$N(h,n)\le 2d\tau(R(h,n))=2d\prod(1+\alpha_p).$$

Proof. All integers m satisfying $(h(m),f(m))=1$ satisfy $h(m)\mid R(h,n)$ by the previous lemma. This leaves at most $\tau(R(h,n))$ possibilities for the value of $|h(m)|$, thus at most $2d\tau(R(h,n))$ possibilities for m. ∎

STATEMENT 3.5. *Assume $1\le d\le n/2$. Let h be a standard polynomial of degree d, and f an integer-valued polynomial of degree n which is a multiple of h. We have*

$$P(f)\le N(h,n)+n^3\le 2d\prod(1+\alpha_p)+n^3.\tag{3.5}$$

Proof. We preserve the notations of the previous lemmas. If $f(m)=q$ is prime, then $aq=af(m)=bh(m)g(m)$ shows that either $g(m)\mid a$ or $h(m)\mid a$ and $(h(m),f(m))=1$. If $g(m)\mid a$, then by Lemma 3.2 we see that $|Gg(m)|\le n!$, and by Lemma 3.1 the number of such m does not exceed

$$2(n-d)n!^{1/(n-d)}+(n-d)\le n^3.$$

(We use $d\le n/2$ and $n!\le n^n2^{1-n}$, which follows from the inequality of arithmetical and geometrical means.) The number of values with $(h(m),f(m))=1$ is at most $N(h,n)$ by definition, and the second inequality is given in the preceding lemma. ∎

This immediately slightly improves the bound $2n\tau(n!)$ of (2.1); a better understanding of $R(h,n)$ could lead to further improvements.

Proof of Theorem 2(i). By Lemma 3.3 and Lemma 3.1 we have

$$N(h,n)\le\#\{m\in\mathbb{Z}:|Hh(m)|\le n!\}\le d(1+2(n!)^{1/d})\le n^{1+n/d}.$$

The claim follows from Statement 3.5. ∎

LEMMA 3.6. *Let g be an integer-valued polynomial. If there are* $\deg g+1$ *consecutive integers at which $g(m)$ is divisible by a certain integer k, then k is a constant divisor of g.*

Proof. After a division, this reduces to the statement that if $\deg g+1$ consecutive values are integral, then so are all the values at integers, which is well known and easily follows from Newton's or Lagrange's interpolation formula. ∎

LEMMA 3.7. *Let h, d, n be as before and let $p > d$ be a prime. If the number of solutions of the congruence*

$$d!h(x) \equiv 0 \pmod{p^{\alpha+1}}$$

is less than $p^{\alpha+1}/(n-d+1)$, then $\alpha_p \le \alpha$.

Proof. By assumption we can find $n-d+1$ consecutive integers for which $p^{\alpha+1} \nmid h(m)$. Thus if $p^{\alpha+1} \mid h(m)g(m)$, then $p \mid g(m)$. Since this holds for $n-d+1 = \deg g + 1$ consecutive integers, by the previous lemma we conclude that p is a constant divisor of g, contrary to assumptions. ∎

Proof of Theorem 2(ii). Let h be a standard polynomial of degree 1 or 2. Write

$$H(x) = 2h(x) = ax^2 + bx + c, \qquad a, b, c \in \mathbb{Z}$$

($a = 0$ is permitted).

We show that for any prime $p > 2$ at least one of the following properties holds:

(a) the congruence $H(x) \equiv 0 \pmod{p^2}$ has at most 2 solutions;

(b) the congruence $H(x) \equiv 0 \pmod{p^3}$ has at most $2p$ solutions, and whenever $p \mid H(m)$, then always $p^2 \mid H(m)$.

Indeed, if $H(x) \equiv 0 \pmod{p^2}$ has no solution at all, we are through. If it has, by a shift we can achieve that 0 is a solution, so we may assume $p^2 \mid c$ and the congruence becomes $x(ax+b) \equiv 0 \pmod{p^2}$. If $p \nmid b$, then p cannot divide both factors, thus either $x \equiv 0 \pmod{p^2}$ or $ax + b \equiv 0 \pmod{p^2}$, at most two solutions altogether. If $p \mid b$, then $p \nmid a$, otherwise p would be a constant divisor of h, contrary to the standardness assumption. In this case $p^2 \mid H(m)$ holds if and only if $p \mid m$, which shows the second claim in (b). To enumerate the solutions modulo p^3, we may assume that 0 is a solution and then we see that any solution satisfies either $x \equiv 0 \pmod{p^2}$, or $ax + b \equiv 0 \pmod{p^2}$, at most $2p$ possibilities modulo p^3.

It can be observed that if $d = 1$, then we always have case (a), and the bound can be reduced to 1.

Let now p be a prime, $\sqrt{2n} < p \le n$. In case (a), we apply Lemma 3.7 with $\alpha = 1$ (d may be 1 or 2), and we obtain $\alpha_p \le 1$. In case (b), we have $d = 2$, and from the same lemma with $\alpha = 2$ we obtain $\alpha_p \le 2$. In both cases whenever $p \mid h(m)$, then $p^{\alpha_p} \mid h(m)$.

Consider now the integers for which $h(m) \mid R(h, n)$. From the above argument, the possible exponents of a prime $\sqrt{2n} < p \le n$ in $h(m)$ are 0 and α_p. For $p \le \sqrt{2n}$ the exponent is $\le n$ by the divisibility $R(h, n) \mid n!$ given in (3.3). This yields at most

$$2(1+n)^{\pi(\sqrt{2n})} 2^{\pi(n) - \pi(\sqrt{2n})}$$

possible values of $h(m)$. By Lemma 3.2 we have

$$N(h,m) \le 2d(1+n)^{\pi(\sqrt{2n})} 2^{\pi(n)-\pi(\sqrt{2n})},$$

and now (3.5) shows (3.2). ∎

4. The lower estimate. We define

$$N'(h,n) = \max_f \min_p \#\{m \in \mathbb{Z} : (h(m), f(m)) = 1,\ p \nmid h(m)\}, \tag{4.1}$$

where f runs over all integer-valued polynomials of degree n which are multiples of h and p runs over the primes.

STATEMENT 4.1. *Let h be an integer-valued polynomial of degree d. For $n > n_0$ (where n_0 depends on d) there is an integer-valued polynomial f of degree n which is divisible by h and for which*

$$P(f) \ge \frac{N'(h,n)}{50(\log n!)^3}.$$

Let $\pi(x,k,l)$ denote the number of primes $\equiv l \pmod k$ not exceeding x.

LEMMA 4.2. *With certain positive absolute constants c, c_1 we have*

$$\pi(x,k,l) = \frac{\operatorname{li} x}{\phi(k)} + O(xe^{-c\sqrt{\log x}})$$

uniformly for all $k \le K$, all $x > \exp(c_1(\log K)^2)$ and all $(l,k) = 1$, except possibly certain values of k which are all multiples of some number k_0 satisfying $k_0 > c(\log K)^2(\log\log K)^{-8}$.

See Karatsuba [1].

Proof of Statement 4.1. Let f_1 be a polynomial for which the expression in (4.1) assumes its maximum. First we deduce bounds for the values of $h(m)$ such that $(h(m), f_1(m)) = 1$.

Let H be the least common denominator of the coefficients of h. By Lemma 3.2 we know that $Hh(m) \mid n!$ for all such m, in particular $1 \le |h(m)| \le n!/H$. We have

$$Hh(x) = a\prod_{i=1}^{d}(x - x_i)$$

with $|a| \ge 1$. Hence these values of m satisfy either $|m - x_1| \le n!$ (we call such values *typical*), or $|m - x_j| < 1$ for some $j \ge 2$ (we call such values *exceptional*). Clearly the number of exceptional m's is less than $2d$. From now on we shall use only the typical m. By a shift (by the integer closest to $\operatorname{Re} x_1$) we can achieve that these satisfy $|m| \le n!$, so we shall assume this inequality.

Next we modify f_1 to make it small at the above values. Write $f_1 = hg_1$. Every polynomial of the form $f_2 = h(g_1 + g^*)$, where $g^* \in \mathbb{Z}[x]$, satisfies the same coprimality assumptions. By choosing the coefficients of g^* appropriately we can achieve that all coefficients of $g_2 = g_1 + g^*$ are in $(0, 1]$. This yields

$$|g_2(m)| \le n(n!)^{n-d}$$

for all typical m, hence

$$|f_2(m)| \le n!|g_2(m)| \le nn!^n.$$

We shall find an f with many prime values in the form $f = f_2 + th$ with an integer t. We will find this t by a statistical argument. We define T by $\log T = (\log n!)^3$. This implies

$$T|h(m)| \ge |f_2(m)|$$

for all typical m. Then we have

$$\#\{t : |t| \le T,\ f_2(m) + th(m) \text{ is prime}\} \ge \pi(T|h(m)|, |h(m)|, |f_2(m)|).$$

By Lemma 4.2 we deduce that this is

$$\ge \frac{1}{2} \cdot \frac{1}{\phi(|h(m)|)} \cdot \frac{T|h(m)|}{\log T|h(m)|} \ge \frac{1}{4} \cdot \frac{T}{\log T}$$

if $h(m)$ is not a multiple of the exceptional k_0. The number of integers m for which this argument works is at least

$$N'(h, n) - 2d.$$

Since the number of choices for t is $\le 2T + 1$, there must be a $|t| \le T$ for which

$$P(f) \ge \frac{1}{2T+1} \cdot \frac{T}{4\log T}(N'(h, n) - 2d).$$

This implies the claim of the statement if $N'(h, n) \ge 6d$. If $1 \le N' < 6d$, then the bound is less than 1 and we can find a prime value simply by applying Dirichlet's theorem; for $N' = 0$ the claim is empty. ∎

Remark 4.3. The difference between $N(h, n)$ and $N'(h, n)$ is of a technical nature and would disappear if we knew that there are no Siegel roots. The denominator in Statement 4.1 is due to the averaging, and the prime-tuple conjecture would give stronger results.

Proof of Theorem 1, lower estimate. We use the above statement for $h(x) = x$. Write $Q = \prod_{p \le n} p$. We set $f = gh/Q$ with

$$g(x) = Qx^{n-1} + \sum_{p \le n} \frac{Q}{p}(x^{p-1} - 1).$$

Clearly g is an integer-valued polynomial of degree $n-1$. Since Q is a constant divisor of $xg(x)$ by Fermat's theorem, f is indeed integer-valued.

Next we show that for every $D \mid Q$ we have $(D, f(D)) = 1$. Indeed, take a prime $q \mid D$. All coefficients of g except those coming from the term $p = q$ in the sum are multiples of q, thus

$$g(D) \equiv \frac{Q}{q}(D^{q-1} - 1) \equiv -\frac{Q}{q} \not\equiv 0 \pmod{q}.$$

Hence

$$(D, f(D)) = \left(D, \frac{g(D)}{Q/D}\right) = 1.$$

This implies

$$\begin{aligned} N'(h,n) &\geq \min_p \#\{m \in \mathbb{Z} : (m, f(m)) = 1,\ p \nmid m\} \\ &\geq \min_p \#\{m \in \mathbb{Z} : m \mid Q,\ p \nmid m\} = 2^{\pi(n)}. \end{aligned}$$

Hence the lower estimate of Theorem 1 follows from Statement 4.1. ■

Acknowledgements. The authors are grateful to the referee for valuable comments and corrections.

References

[1] A. A. Karatsuba, *Basic Analytic Number Theory*, Springer, New York, 1993.

Department of Mathematics
Nanjing Normal University
Nanjing 210097, Jiangsu, P.R. China
E-mail: ygchen@pine.njnu.edu.cn

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
Budapest, Pf. 127, H-1364 Hungary
E-mail: ruzsa@renyi.hu

Received on 3.2.1999
and in revised form on 20.3.2000 (3553)